



**OfficeConnect®**

Cable/DSL Secure Gateway (3CR856-95)

User Guide



**3Com Corporation**  
**5400 Bayfront Plaza**  
**Santa Clara, California 95052-8145**

Copyright © 2002, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Technologies.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

**UNITED STATES GOVERNMENT LEGEND**

*If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:*

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo and OfficeConnect are registered trademarks of 3Com Corporation.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

Netscape Navigator is a registered trademark of Netscape Communications.

JavaScript is a trademark of Sun Microsystems

All other company and product names may be trademarks of the respective companies with which they are associated.

**ENVIRONMENTAL STATEMENT**

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

**End of Life Statement**

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

**Regulated Materials Statement**

3Com products do not contain any hazardous or ozone-depleting material.

**Environmental Statement about the Documentation**

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

# CONTENTS

## Contents 3

### About This Guide 7

- Naming Convention 7
- Conventions 7

### Introducing the OfficeConnect Cable/DSL Secure Gateway 9

- OfficeConnect Cable/DSL Secure Gateway 9
- Cable/DSL Secure Gateway Advantages 10
- Package Contents 11
- Minimum System and Component Requirements 11
- Front Panel 12
- Rear Panel 13

### Installing the Gateway 15

- Introduction 15
- Positioning the Gateway 15
  - Safety Information 15
  - Using the Rubber Feet 15
- Before you Install your Gateway 15
  - PPPoE 16
  - PPTP 16
  - DHCP 16
  - Static 16
- Powering Up the Gateway 17
- Connecting the Cable/DSL Secure Gateway 17

### Setting Up Your Computers 19

- Obtaining an IP Address Automatically 19
  - Windows 2000, XP 19
  - Windows 95, 98, ME 20
  - Macintosh OS 8.5, 9.x 20
- Disabling PPPoE and PPTP Client Software 20

### Running the Setup Wizard 23

- Accessing the Wizard 23
- Setting the Password 24
- Setting the Time Zone 25
- Auto-Configuration Settings 26
- Internet Settings 26
- Choosing your LAN Settings 30
- Activating DHCP 30
- Viewing the Summary 31

### Gateway Configuration 33

- Navigating Through the Gateway Configuration Pages 33
  - Main Menu 33
  - Option Tabs 33
- Welcome Screen 34
  - Viewing the Notice Board 34
  - Changing the Administration Password 34
  - Setup Wizard 35

LAN Settings	35
LAN IP Settings	35
DHCP Clients List	37
Internet Settings	38
Connection to ISP	39
Setting up NAT	43
Configuring the Firewall	45
The Virtual Servers Menu	45
PC Privileges	47
Special Applications	49
Advanced	52
Configuring VPNs	53
Setting the VPN Mode	53
Viewing VPN Connections	55
Editing IPSec Routes	60
Accessing the System Tools	61
Restart	61
Time Zone	62
Loading and Saving the Gateway Configuration	62
Upgrading the Firmware of your Gateway	63
Viewing Status and Logs	64
Obtaining Support and Feedback for your Gateway	65

## **Troubleshooting 67**

Basic Connection Checks	67
Browsing to the Gateway Configuration Screens	67
Connecting to the Internet	68

Forgotten Password	68
Alert LED	69
Recovering from Corrupted Software	69
Frequently Asked Questions	70

## **Using Discovery 71**

Running the Discovery Application	71
Windows Installation (95/98/2000/Me/NT)	71

## **IP Addressing 73**

The Internet Protocol Suite	73
How does a Device Obtain an IP Address and Subnet Mask?	74
DHCP Addressing	74
Static Addressing	74
Auto-IP Addressing	75
Private IP Addresses	75

## **Technical Specifications 77**

Interfaces	77
Operating Temperature	77
Power	77
Humidity	77
Dimensions	77
Weight	77
Standards	77
System Requirements	78
Operating Systems	78
Ethernet Performance	78

Cable Specifications 78

**Safety Information 79**

Important Safety Information 79

Wichtige Sicherheitshinweise 79

Consignes importantes de sécurité 80

**End User Software Licence Agreement 83**

3Com Corporation

END USER SOFTWARE LICENSE AGREEMENT 83

**ISP Information 85**

Information Regarding Popular ISPs 85

**Glossary 87**

**Index 93**

**Regulatory Notices 99**



# ABOUT THIS GUIDE

This guide is intended for use by those responsible for installing and setting up network equipment; consequently, it assumes a basic working knowledge of LANs (Local Area Networks) and Internet gateway systems.



*If a release note is shipped with this OfficeConnect Cable/DSL Secure Gateway and contains information that differs from the information in this guide, follow the information in the release note.*

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) on the 3Com World Wide Web site:

<http://www.3com.com>

## Naming Convention

Throughout this guide, the *OfficeConnect Cable/DSL Secure Gateway* is referred to as the *Gateway*.

Category 3 and Category 5 Twisted Pair Cables are referred to as Twisted Pair Cables throughout this guide.

## Conventions

[Table 1](#) and [Table 2](#) list conventions that are used throughout this guide.

**Table 1** Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
	Warning	Information that alerts you to potential personal injury

**Table 2** Text Conventions

Convention	Description
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del

**Table 2** Text Conventions (continued)

Convention	Description
Words in <i>italics</i>	Italics are used to: <ul style="list-style-type: none"><li>■ Emphasize a point.</li><li>■ Denote a new term at the place where it is defined in the text.</li><li>■ Identify menu names, menu commands, and software button names. Examples: From the <i>Help</i> menu, select <i>Contents</i>. Click <i>OK</i>.</li></ul>

## Feedback about this User Guide

Your suggestions are very important to us. They will help make our documentation more useful to you. Please e-mail comments about this document to 3Com at:

**[pddtechpubs\\_comments@3com.com](mailto:pddtechpubs_comments@3com.com)**

Please include the following information when commenting:

- Document title
- Document part number (on the title page)
- Page number (if appropriate)

Example:

- OfficeConnect Cable/DSL Secure Gateway User Guide
- Part Number DUA08569-5AAA02
- Page 24



*Do not use this e-mail address for technical support questions. For information about contacting Technical Support, please refer to the Support and Safety Information sheet.*

## Related Documentation

In addition to this guide, each OfficeConnect Cable/DSL Secure Gateway document set includes one Installation Guide. This guide contains the instructions you need to install and configure your Cable/DSL Secure Gateway.

## Product Registration

You can now register your OfficeConnect Cable/DSL Secure Gateway on the 3Com web site and receive up-to-date information on your product:

**<http://www.3com.com/register>**



# INTRODUCING THE OFFICECONNECT CABLE/DSL SECURE GATEWAY

Welcome to the world of networking with 3Com®. In the modern business environment, communication and sharing information is crucial. Computer networks have proved to be one of the fastest modes of communication but, until recently, only large businesses could afford the networking advantage. The OfficeConnect® product range from 3Com has changed all this, bringing networks to the small office.

The products that compose the OfficeConnect line give you, the small office user, the same power, flexibility, and protection that has been available only to large corporations. Now, you can network the computers in your office, connect them all to a single Internet outlet, and harness the combined power of all of your computers.

---

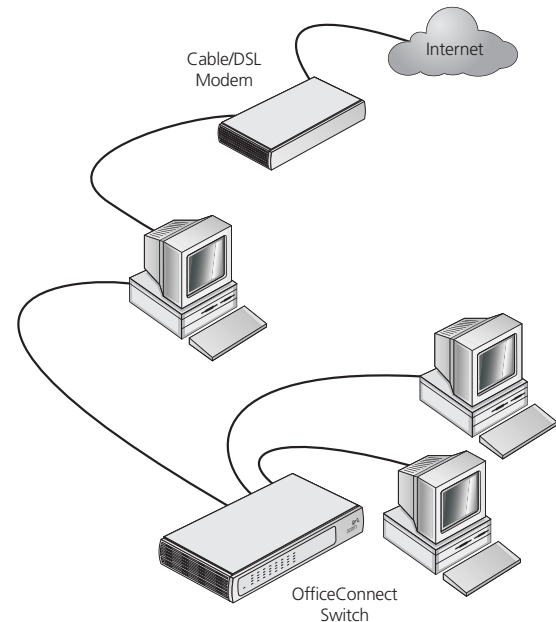
## OfficeConnect Cable/DSL Secure Gateway

The OfficeConnect Cable/DSL Secure Gateway is designed to provide a cost-effective means of sharing a single broadband Internet connection amongst several computers.

The Gateway also increases your network security by acting as a firewall — preventing unauthorised external access to your network — and by creating Virtual Private Networks (VPNs) — encrypted links to other private networks.

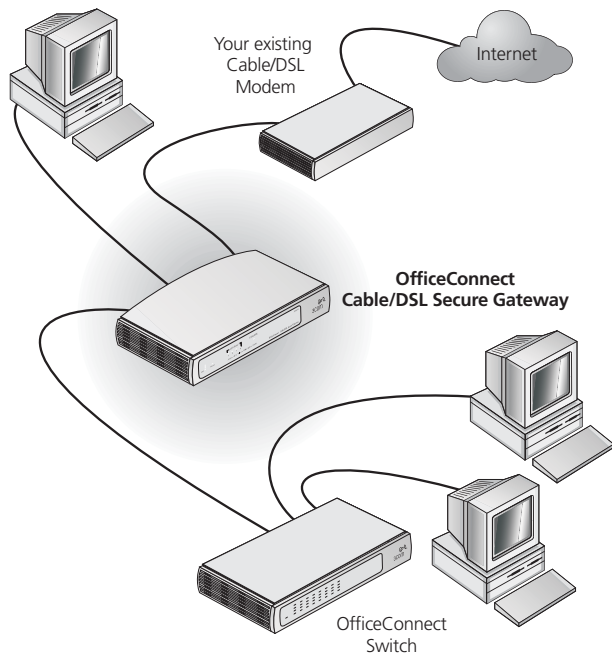
The example in [Figure 1](#) shows a network connected to the Internet without a Gateway. One computer is connected to the Internet using a Cable or DSL modem. This computer must always be powered on for the other computers on the network to access the Internet.

**Figure 1** Example Network Without a Cable/DSL Secure Gateway



When you use the Cable/DSL Secure Gateway in your network ([Figure 2](#)), it becomes your connection to the Internet. Connections can be made directly to the Gateway, or through an OfficeConnect Hub or Switch, expanding the number of computers you can have in your network.

**Figure 2** Example Network Using a Cable/DSL Secure Gateway



---

## Cable/DSL Secure Gateway Advantages

The advantages of using a Gateway include:

- Shared Internet connection.
- No need for a dedicated, “always on” computer serving as your Internet connection.
- Cross-platform operation for compatibility with Windows, Unix and Macintosh computers.
- Easy-to-use, Web-based setup and configuration.
- Provides centralization of all network address settings (DHCP).
- Provides *Virtual Server* redirection to enable remote access to Web, FTP, and other services on your network
- Provides firewall protection against Internet hacker attacks.
  - Implements Stateful Packet Inspection to block network intrusions.
  - Blocks Denial of Service attacks by using pattern detection.
- Supports Virtual Private Networks (VPNs).
  - Initiates and terminates IPSec connections.
  - Terminates PPTP and L2TP over IPSec connections.
  - Provides hardware accelerated encryption for IPSec VPNs, including L2TP over IPSec.

---

## Package Contents

The OfficeConnect Cable/DSL Secure Gateway kit includes the following items:

- One OfficeConnect Cable/DSL Secure Gateway
- One power adapter for use with the Gateway
- Four rubber feet
- One stacking clip
- One Ethernet cable
- One CD-ROM containing
  - the Gateway Discovery program
  - a backup copy of the Gateway firmware
  - the Installation Guide
  - this User Guide
- Installation Guide
- One Support and Safety Information Sheet
- One Warranty Flyer
- One License Agreement
- This User Guide

If any of these items are missing or damaged, please contact your retailer.

---

## Minimum System and Component Requirements

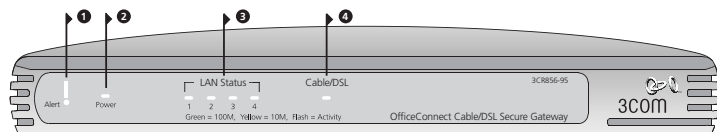
Your OfficeConnect Cable/DSL Secure Gateway requires that the computer(s) and components in your network be configured with at least the following:

- A computer with an operating system that supports TCP/IP networking protocols (for example Windows 95/98/NT/Me/2000/XP, Unix, Mac OS 8.5 or higher).
- An Ethernet 10 Mbps or 10/100 Mbps NIC for each computer to be connected to the four-port switch on your Gateway.
- A cable modem or DSL modem with an Ethernet port (RJ-45 connector).
- An active Internet access account.
- A Web browser program that supports JavaScript, such as Netscape 4.7 or higher or Internet Explorer 5.5 or higher.

## Front Panel

The front panel of the Gateway contains a series of indicator lights (LEDs) that help describe the state of various networking and connection operations.

**Figure 3** Cable/DSL Secure Gateway - Front Panel



### 1 Alert LED (Orange)

Indicates a number of different conditions, as described below.

**Off** The Gateway is operating normally.

**Flashing quickly** Indicates one of the following conditions:

- The Gateway has just been started up and is running a self-test routine.
- The system software is in the process of being upgraded.

In each of these cases, wait until the Gateway has completed the current operation and the alert LED is Off.

### Flashing slowly (Two seconds on, two seconds off)

The Gateway has completed the Reset to Factory Defaults process, and is waiting for you to reset the unit. To do this, remove power, wait 10 seconds and then re-apply power. The Gateway will then enter the start-up sequence and resume

normal operation. See [“Recovering from Corrupted Software”](#) on [page 69](#).

**On for 2 seconds, and then off** The Gateway has detected and prevented a hacker from attacking your network from the Internet.

**Continuously on** A fault has been detected with your Gateway during the start-up process. See [“Troubleshooting”](#) on [page 67](#).



*The Alert LED will be on for a period of between three and five seconds during the power on self test. This is normal and no cause for alarm.*

### 2 Power LED (Green)

Indicates that the Gateway is powered on.

### 3 Four LAN Status LEDs

#### Green (100 Mbps link) / Yellow (10 Mbps link)

Indicates a number of different conditions, as described below.

**On** The link between the port and the next piece of network equipment is OK.

**Flashing** The link is OK and data is being transmitted or received.

**Off** Indicates one of the following

- nothing is connected

- the connected device is switched off
- there is a problem with the connection. [“Troubleshooting” on page 67.](#)

## 4 Cable/DSL Status LED

### Green (100 Mbps link) / Yellow (10 Mbps link)

Indicates a number of different conditions, as described below.

**On** The link between the Gateway and the cable or DSL modem is OK.

**Flashing** The link is OK and data is being transmitted or received.

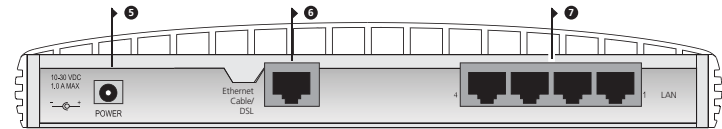
**Off** Indicates one of the following

- nothing is connected
- the modem is switched off
- there is a problem with the connection. [“Troubleshooting” on page 67.](#)

## Rear Panel

The rear panel ([Figure 4](#)) of the Gateway contains four LAN ports, one Ethernet Cable/DSL port, and a power adapter socket.

**Figure 4** Cable/DSL Secure Gateway - Rear Panel



## 5 Power Adapter socket

Only use the power adapter that is supplied with this Gateway. Do not use any other adapter.

## 6 Ethernet Cable/DSL port

Use the supplied patch cable to connect the Gateway to the 10/100 port on your cable or DSL modem. This port will automatically adjust for the correct speed, duplex and cable type. You can connect your Cable/DSL modem using either straight-through or crossover cables.

## 7 Four 10/100 LAN ports

Use suitable cable with RJ-45 connectors. You can connect your Gateway to a computer, or to any other piece of equipment that has an Ethernet connection (for example, a hub or a switch). All ports will automatically adjust for the correct speed, duplex and cable type. You can connect your Ethernet devices using either straight-through or crossover cables.



# INSTALLING THE GATEWAY

---

## Introduction

This chapter will guide you through a basic installation of the OfficeConnect Cable/DSL Secure Gateway, including:

- Connecting the Gateway to the Internet.
- Connecting the Gateway to your network.

---

## Positioning the Gateway

You should place the Cable/DSL Secure Gateway in a location that:

- is conveniently located for connection to the cable or DSL modem that will be used to connect to the Internet.
- allows convenient connection to the computers that are to be connected to the four LAN ports on the rear panel.
- allows easy viewing of the front panel LED indicator lights, and access to the rear panel connectors, if necessary.

## Safety Information



**WARNING:** Please read the “Important Safety Information” section in Appendix D before you start.



**VORSICHT:** Bitte lesen Sie den Abschnitt “Wichtige Sicherheitsinformationen” sorgfältig durch, bevor Sie das Gerät einschalten.



**AVERTISSEMENT:** Veuillez lire attentivement la section “Consignes importantes de sécurité” avant de mettre en route.

When positioning your Gateway, ensure:

- It is out of direct sunlight and away from sources of heat.
- Cabling is away from power lines, fluorescent lighting fixtures, and sources of electrical noise such as radios, transmitters and broadband amplifiers.
- Water or moisture cannot enter the case of the unit.
- Air flow around the unit and through the vents in the side of the case is not restricted. We recommend you provide a minimum of 25mm (1in.) clearance.

## Using the Rubber Feet

Use the four self-adhesive rubber feet to prevent your Gateway from moving around on your desk or when stacking with flat top OfficeConnect units. Only stick the feet to the marked areas at each corner of the underside of your Gateway.

---

## Before you Install your Gateway

Before you install and configure your Gateway, you need the following additional information. If you do not have this information, contact your Internet Service Provider or see [“ISP Information”](#) on [page 85](#) for details of popular ISPs. Space is provided below for you to record this information.

## PPPoE

If your ISP allocates IP information dynamically over PPPoE, you need a User Name and Password:

PPPoE User Name: \_\_\_\_\_

PPPoE Password: \_\_\_\_\_

PPPoE Service Name: \_\_\_\_\_

Host Name: \_\_\_\_\_

## PPTP

If your ISP allocates IP information dynamically over PPTP, you need a User Name and Password

PPTP User Name: \_\_\_\_\_

PPTP Password: \_\_\_\_\_

PPTP Server Address: \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_



*Only enter a PPPoE Service Name or Host Name or a PPTP Server Address if your ISP requires you to do this. Do not enter anything if your ISP does not require a service name*

## DHCP

If your ISP allocates IP information dynamically using DHCP they may require you to use keep a fixed MAC Address and Host Name for security purposes.

MAC Address: \_\_\_\_\_

Host Name: \_\_\_\_\_

## Static

If your ISP allocates fixed or static IP information, you need the following information:

IP Address: \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_

Subnet Mask: \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_

Default Gateway Address: \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_

Primary DNS Address: \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_



---

## Powering Up the Gateway

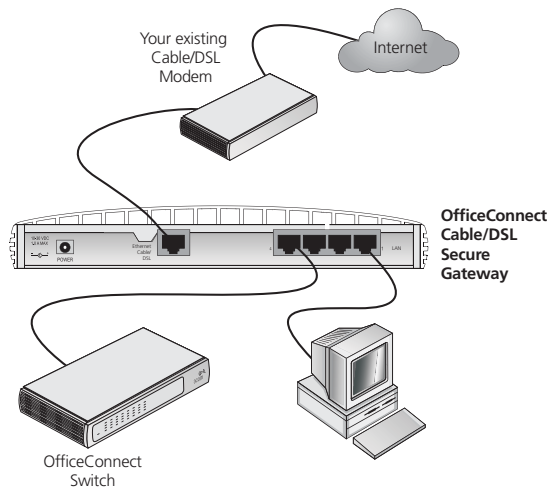
- 1 Plug the power adapter into the power adapter socket located on the back panel of the Gateway (refer to [“Power Adapter socket”](#) on [page 13](#)).
- 2 Plug the power adapter into a standard electrical wall socket.

---

## Connecting the Cable/DSL Secure Gateway

The first step for installing your Cable/DSL Secure Gateway is to physically connect it to a cable or DSL modem in order to be able to access the Internet.

**Figure 5** Connecting the Cable/DSL Secure Gateway



To use your Cable/DSL Secure Gateway to connect to the Internet through an external cable or DSL modem ([Figure 5](#)):

- 1 Use the supplied cable to connect the Gateway's Ethernet Cable/DSL port to your Cable/DSL modem. Ensure that your modem is connected to the Internet and switched on.
- 2 Connect your computer to one of the 10/100 LAN ports on the Gateway.
- 3 Connect the power adaptor to the Gateway and wait for the Alert LED to stop flashing. Check that the Cable/DSL Status LED is illuminated.
- 4 Switch on your computer. Once your computer is ready to use, check that the LAN Port Status LED on the Gateway is illuminated.

You have now completed the hardware installation of your Gateway. You now need to set up your computers so that they can make use of the Gateway to communicate with the Internet.



# SETTING UP YOUR COMPUTERS

The OfficeConnect Cable/DSL Secure Gateway has the ability to dynamically allocate network addresses to the computers on your network, using DHCP. However, your computers need to be configured correctly for this to take place. To change the configuration of your computers to allow this, follow the instructions in this chapter.

If your computers are configured with static addresses (also known as fixed addresses) and you do not wish to change this, then you should use the Discovery program on the Gateway CD-ROM to detect and configure your Gateway. Refer to [“Using Discovery”](#) on [page 71](#) for information on using the Discovery program.

---

## Obtaining an IP Address Automatically

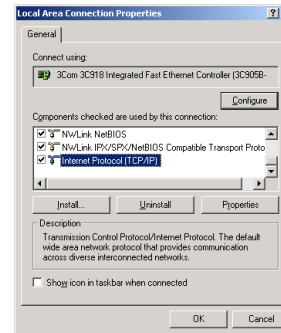
### Windows 2000, XP

If you are using a Windows 2000 or Windows XP computer, use the following procedure to change your TCP/IP settings (Windows XP specific instructions in brackets):

- 1 From the Windows *Start* Menu, select *Settings > Control Panel* (select Control Panel directly from the Start menu in Windows XP)
- 2 Double click on *Network and Dial-Up Connections* (*Network and Internet Connections*). For XP only — click on *Network Connections*.
- 3 Double click on *Local Area Connection*.
- 4 Click on *Properties*.

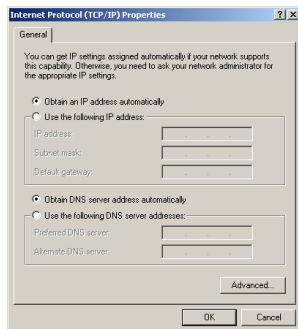
- 5 A screen similar to [Figure 6](#) should be displayed. Select *Internet Protocol (TCP/IP)* and click on *Properties*.

**Figure 6** Local Area Connection Properties



- 6 Ensure that the options *Obtain an IP Address automatically*, and *Obtain DNS server address automatically* are both selected as shown in [Figure 7](#). Click OK.

**Figure 7** Internet Protocol Properties



- 7 Restart your computer.

## Windows 95, 98, ME

- 1 From the Windows *Start* Menu, select *Settings > Control Panel*.
- 2 Double click on *Network*. Select the *TCP/IP* item for your network card and click on *Properties*.
- 3 In the *TCP/IP* dialog, select the *IP Address* tab, and ensure that *Obtain IP address automatically* is selected. Click *OK*.
- 4 Restart your computer.

## Macintosh OS 8.5, 9.x

If you are using a Macintosh computer, use the following procedure to change your *TCP/IP* settings:

- 1 From the desktop, select *Apple Menu, Control Panels*, and *TCP/IP*.
- 2 In the *TCP/IP* control panel, set *Connect Via:* to "Ethernet."

- 3 In the *TCP/IP* control panel, set *Configure:* to "Using DHCP Server."
- 4 Close the *TCP/IP* dialog box, and save your changes.
- 5 Restart your computer.

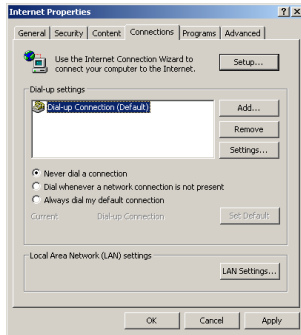
---

## Disabling PPPoE and PPTP Client Software

If you have PPPoE or PPTP client software installed on your computer, you will need to disable it. To do this:

- 1 From the Windows *Start* menu, select *Settings > Control Panel*.
- 2 Double click on *Internet Options*.
- 3 Select the *Connections* Tab. A screen similar to [Figure 8](#) should be displayed.
- 4 Select the *Never Dial a Connection* option and click *OK*.

**Figure 8** Internet Properties



*You may wish to remove the PPPoE client software from your computer to free resources, as it is not required for use with the Gateway.*

---

## Disabling Web Proxy

Ensure that you do not have a web proxy enabled on your computer.

Go to the *Control Panel* and click on *Internet Options*. Select the *Connections* tab and click on *LAN Settings* at the bottom. Make sure that the *Use Proxy Server* option is unchecked.



# RUNNING THE SETUP WIZARD

If the Gateway needs to be configured, for example if it has not yet been used or has been reset, it will run the Setup Wizard automatically. This detects some of the settings the Gateway needs to function and asks that you input the others.

## Accessing the Wizard

The Cable/DSL Secure Gateway Setup Wizard is Web-based, which means that it is accessed through your Web browser (Netscape Navigator or Internet Explorer).

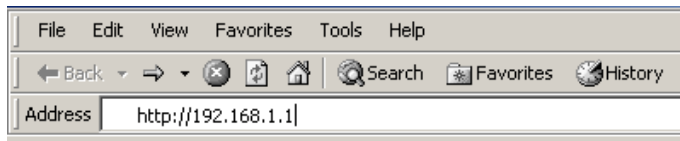
To use the Setup Wizard:

- 1 Ensure that you have at least one computer connected to the Gateway. See [“Installing the Gateway”](#) on [page 15](#).
- 2 Launch your Web browser on the computer. Enter the URL of your Gateway in to the location or address box of your browser ([Figure 9](#)).



The default URL for the gateway is **http://192.168.1.1**. If you have changed the IP address of the unit you should substitute this for the default address within the URL.

**Figure 9** Web Browser Location Field (Factory Default)



The *Login* screen, as shown in [Figure 10](#), should appear in your browser. If it does not, refer to [“Troubleshooting”](#) on [page 67](#).

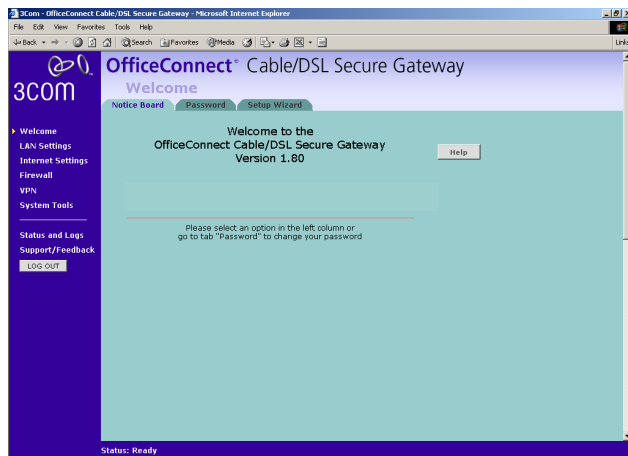
- 3 To log in, enter the password (the default password is *admin*) in the *System Password* field and click *Log in*.

**Figure 10** Login Screen



- 4 If the password is correct, the *OfficeConnect Cable/DSL Secure Gateway Welcome* screen, shown in [Figure 11](#), will appear. If your Gateway has not been configured before, the Wizard, shown in [Figure 12](#), will also launch automatically.

**Figure 11** Welcome Screen



If the *Wizard* does not launch automatically (this may occur if the Gateway has been powered up or configured previously) you can launch the *Wizard* manually.

- 5 To launch the *Wizard* manually click on the *Setup Wizard* tab in the welcome screen followed by the *WIZARD...* button.

**Figure 12** Wizard Screen



Click *Next* to continue.

You will now be guided through the setup of your Gateway.

## Setting the Password

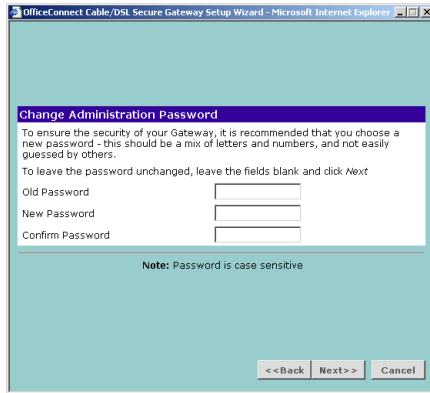
When the *Change Administration Password* screen ([Figure 13](#)) appears, type the *Old Password*, then a new password in both the *New Password* and *Confirm Password* fields.



*The default password for the Gateway is 'admin'. It is case sensitive and must be entered as the Old Password the first time you configure the Gateway. 3Com recommends that you change the password from its default value.*



**Figure 13** Change Administration Password Screen



*Choose a password that you can remember but that others are unlikely to guess. Remember that the password is case sensitive.*

Click **Next** to display the *Time Zone* setup screen ([Figure 14](#)).

## Setting the Time Zone

The Gateway sets its time automatically when it connects to the Internet. This time is used when recording information log files.

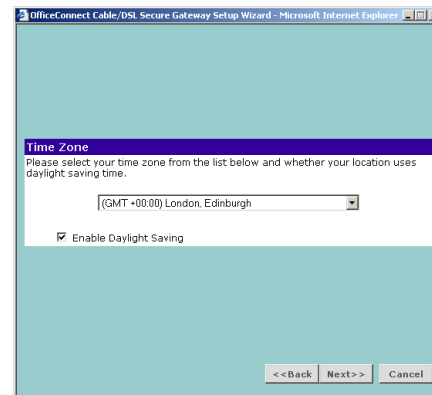
To set the Gateway to your local time:

- 1 Select your time zone from the drop-down menu.
- 2 Check the *Enable Daylight Saving* box to automatically adjust the time seasonally.
- 3 Click **Next** to continue.

To set the Gateway to World Time (UTC):

- 1 Select *(GMT) Greenwich Mean Time* from the drop-down menu.
- 2 Ensure that the *Enable Daylight Saving* box is cleared.
- 3 Click **Next** to continue.

**Figure 14** Time Zone Screen

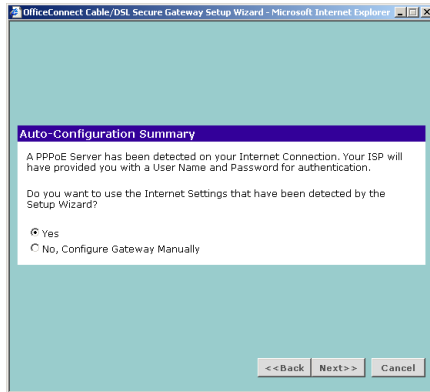


*The Daylight Savings option automatically adjusts the system clock for summer and winter time. To disable this feature ensure that the **Enable Daylight Saving** box is cleared.*

## Auto-Configuration Settings

If the Gateway is able to detect a PPPoE or DHCP server on its Ethernet Cable/DSL port then it will offer you the option of configuring its Internet settings automatically. As an example, the *Auto-Configuration* screen for PPPoE is shown in [Figure 15](#) below.

**Figure 15** PPPoE Auto-configuration Screen



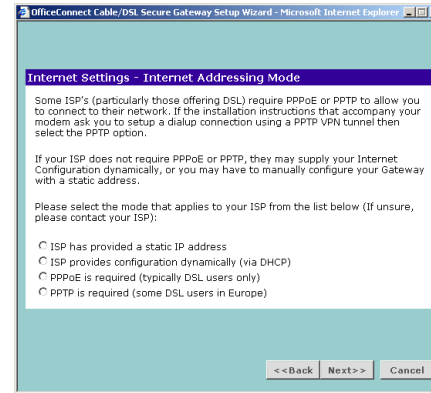
Click *Next* to accept the option you have chosen and continue.

- If the Gateway could not automatically configure your internet settings or if you chose to configure your Internet settings manually, continue at [“Internet Settings”](#) below.
- If you chose one of the automatic configuration options continue at [“Choosing your LAN Settings”](#) on [page 29](#).

## Internet Settings

The *Internet Settings* window allows you to set up the Gateway for the type of Internet connection you have. Before setting up your Internet connection mode, have the modem configuration supplied by your ISP to hand.

**Figure 16** Internet Settings Screen



Select the Internet Addressing mode your ISP requires and click *Next*. Depending on your selection, refer to:

- [“Static IP Mode”](#) on [page 27](#)
- [“Dynamic IP Address Mode”](#) on [page 27](#)
- [“PPPoE Mode”](#) on [page 28](#).
- [“PPTP Mode”](#) on [page 29](#).

## Static IP Mode

To setup the Gateway for use with a static IP address connection, use the following procedure:


**Figure 17** Static IP Mode Screen

- 1 Enter your IP Address in the *IP Address* text box.
- 2 Enter your subnet mask in the *Subnet Mask* text box.
- 3 Enter your ISP gateway address in the *Internet (ISP) Gateway Address* text box.
- 4 Enter your primary DNS address in the *Primary DNS Address* text box.
- 5 If your ISP provides a secondary DNS address, enter it in the *Secondary DNS Address* text box, otherwise leave the box blank.
- 6 Click *Next* to continue.

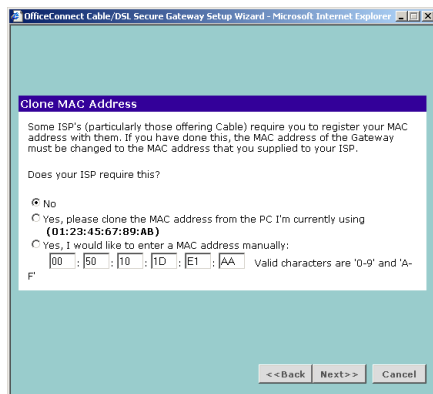
## Dynamic IP Address Mode

To setup the Gateway for use with a dynamic IP address connection:

**Figure 18** Hostname Screen

- 1 If your ISP requires the addresses of a Primary and Secondary DNS Server then enter them in the fields labelled *Primary DNS Address* and *Secondary DNS Address*.  
 *If your ISP does not require one of the fields to be filled in then leave it blank. This indicates to the Gateway that there is no server.*
- 2 If your ISP requires you to supply a host name enter it in the *Host Name* box, otherwise leave the box blank.
- 3 Click *Next* to continue to the *Clone MAC Address* screen, shown in [Figure 19](#) below.

**Figure 19** Clone MAC Address Screen



- 4 If your ISP requires an assigned MAC address, select the appropriate radio button:
  - *Yes, please clone the MAC address from the PC I'm currently using* if the computer you are using now is the one that was previously connected directly to the cable or DSL modem.
  - *Yes, I would like to enter a MAC address manually* and manually enter the values for a MAC address if the computer you are using now was **not** previously connected directly to the cable or DSL modem.

Otherwise click *No*.

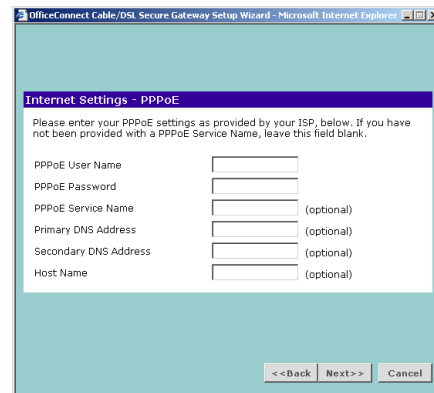
- 5 Click *Next* to continue

Continue at [“Choosing your LAN Settings”](#) on [page 30](#).

## PPPoE Mode

To setup the gateway for use with a PPP over Ethernet (PPPoE) connection, use the following procedure:

**Figure 20** PPPoE Screen



- 1 Enter your PPP over Ethernet user name in the *PPPoE User Name* text box.
- 2 Enter your PPP over Ethernet password in the *PPPoE Password* text box.



*If your ISP does not require one of the fields to be filled in then leave it blank. This indicates to the Gateway that there is no server.*

- 3 If your ISP requires you to supply a PPPoE service name, enter it in the *PPPoE Service Name* text box.

- 4 If your ISP requires the addresses of a Primary and Secondary DNS Server then enter them in the fields labelled *Primary DNS Address* and *Secondary DNS Address*.
- 5 If your ISP requires you to supply a host name enter it in the *Host Name* box, otherwise leave the box blank.
- 6 Click *Next* to continue.

Continue at ["Choosing your LAN Settings"](#) on [page 30](#).

## PPTP Mode

To setup the gateway for use with a PPTP connection, use the following procedure:

**Figure 21** PPTP Screen

OfficeConnect Cable/DSL Secure Gateway Setup Wizard - Microsoft Internet Explorer

### Internet Settings - PPTP Mode

Please enter your PPTP account settings, as provided by your ISP, below.

The PPTP Server is typically located in your DSL modem. In the case of an Alcatel Speed Touch modem, its default address is 10.0.0.138

PPTP Server Address:

PPTP User Name:

PPTP Password:

Primary DNS Address:  (optional)

Secondary DNS Address:  (optional)

<<Back Next>> Cancel

- 1 Enter your PPTP server address in the *PPTP Server Address* text box.

- 2 Enter your PPTP user name in the *PPTP User Name* text box.
- 3 Enter your PPTP password in the *PPTP Password* text box.
- 4 Enter your primary DNS address in the *Primary DNS Address* text box.
- 5 If your ISP provides a secondary DNS address, enter it in the *Secondary DNS Address* text box, otherwise leave the box blank.
- 6 Check all your settings, and then click *Next*. [Figure 22](#) displays.
- 7 Click *Next* to continue.

**Figure 22** PPTP IP Settings

OfficeConnect Cable/DSL Secure Gateway Setup Wizard - Microsoft Internet Explorer

### Internet Settings - PPTP Mode

You must specify some IP settings to be used when establishing the PPTP connection. If your ISP has provided you with these settings, then you should use them. Otherwise, if the PPTP server is located in your DSL modem, you can use the Suggest button to generate suitable values for you.

Initial IP Address:

Initial Subnet Mask:

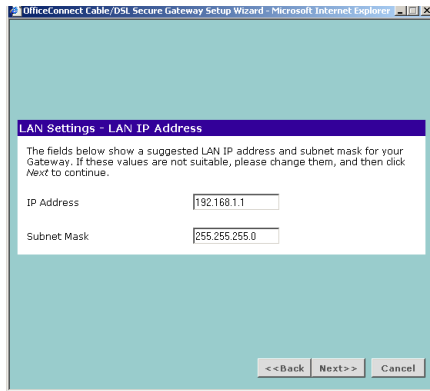
<<Back Next>> Cancel

- 8 IP settings must be used when establishing a PPTP connection. Fill in the *Initial IP Address* and the *Initial Subnet Mask* fields if your ISP has provided you with these settings. Alternatively, if the PPTP server is located in your DSL modem, click *Suggest* to select and IP address on the same subnet as the PPTP server.

## Choosing your LAN Settings

The LAN settings screen, shown in [Figure 23](#) below, displays the Gateway's current IP address and subnet mask. If this is the first time the Wizard has been run it will display the default address and subnet mask.

**Figure 23** LAN IP Address Screen



OfficeConnect Cable/DSL Secure Gateway Setup Wizard - Microsoft Internet Explorer

**LAN Settings - LAN IP Address**

The fields below show a suggested LAN IP address and subnet mask for your Gateway. If these values are not suitable, please change them, and then click Next to continue.

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

<< Back   Next >>   Cancel

- 1 Enter your chosen IP address for the Gateway in the *IP Address* field. This should be a private network so that it does not conflict with IP addresses on the Internet. See [“Private IP Addresses” on page 75](#).



3Com recommends that you use the default IP address and subnet mask unless you already have a network that uses different values.

- 2 Enter your chosen subnet mask in the Subnet Mask field. This should be large enough to contain all your computers and other network devices. The default (255.255.255.0) allows for 254 devices including the Gateway.



*If you are going to set up an IPSec VPN with another Gateway you must set your subnet mask to 255.255.255.0. See [“Configuring VPNs” on page 53](#).*

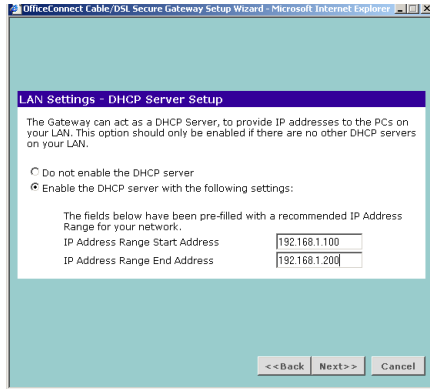
## Activating DHCP

The Gateway contains a Dynamic Host Configuration (DHCP) server that can automatically configure the TCP/IP settings of every computer on your network. The *DHCP Server Setup* screen is shown below.



*If you intend to use the Gateway to control the permissions of individual machines on your network then you must use the Gateway's DHCP server to allocate addresses or use static addressing. If you use another DHCP server you may get unexpected results. See [“PC Privileges” on page 47](#).*

**Figure 24** DHCP Server Setup Screen



*3Com recommends that you activate the DHCP server and leave it at the default values unless you already have a DHCP Server on your network.*

- To activate the DHCP Server option, select *Enable the DHCP server with the following settings*. The DHCP server will default to the addresses 192.168.1.100 to 192.168.1.200 if the IP address of the Gateway has been left at the default 192.168.1.1.



*The Setup Wizard suggests a DHCP server address range that is valid for the LAN settings entered. If the defaults are used it will be .100 - .200. The suggested range will vary depending on the LAN settings entered in the LAN IP Address screen.*

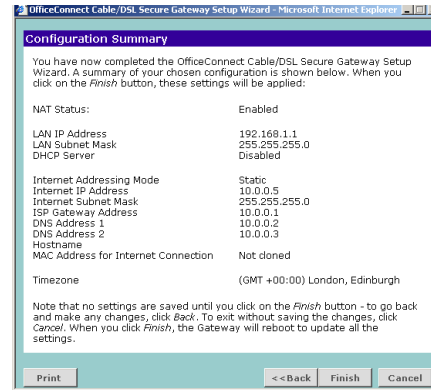
- To disable DHCP, select *Do not enable the DHCP server*.

Click *Next* when you have finished.

## Viewing the Summary

When you complete the Setup Wizard, a configuration summary will display. See [Figure 25](#) below. Verify the configuration information of the Gateway and click *Finish* to save your settings and restart the Gateway.

**Figure 25** Configuration Summary Screen



*3Com recommends that you print the Configuration Summary screen for your records.*



*If you have changed the IP address of your Gateway your computer will need to change its IP address to communicate with the Gateway. Reboot your computer once the Gateway has restarted to get a new address.*

If want to make changes, click the *Back* button until you reach the screen which contains the settings you want to change and follow the instructions from that point.

Your Gateway is now configured.

You can start using your Gateway straight away or further configure your Gateway (see [“Gateway Configuration”](#) on [page 33](#)).



# GATEWAY CONFIGURATION

This chapter describes all the options available through the Gateway configuration pages, and is provided as a reference.

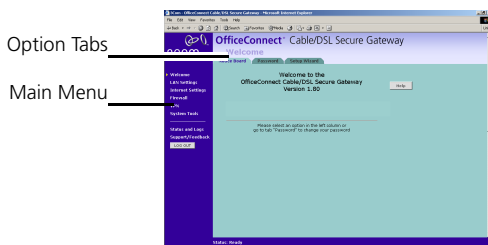
## Navigating Through the Gateway Configuration Pages

To get to the configuration pages, browse to the Gateway by entering the URL in the location bar of your browser. The default URL is `http://192.168.1.1`. If you changed the Gateway LAN IP address during initial configuration, use the new IP address instead. When you have browsed to the Gateway, log in using your system password. The default password is 'admin'.

### Main Menu

At the left side of all screens is a main menu, as shown in [Figure 26](#). When you click on a topic from the main menu, that page will appear in the main part of the screen.

**Figure 26** OfficeConnect Cable/DSL Secure Gateway Screen Layout



- **Welcome** — displays the firmware version of the Gateway and important messages on the Notice Board, allows you to change your password, and launch the Wizard.

- **LAN Settings** — allows you to configure IP address and subnet mask information, set up DHCP server parameters, and display the DHCP client list.
- **Internet Settings** — sets up Internet addressing modes such as PPPoE connection, dynamic IP address allocation, Network Address Translation (NAT) and static IP address settings.
- **Firewall** — allows configuration of the Gateway's firewall features: Virtual Servers, Special Applications, PC Privileges and other general security options.
- **VPN** — Allows the administrator to set up and maintain Virtual Private Network (VPN) connections.
- **System Tools** — allows the administrator to perform maintenance activities on the Gateway.
- **Status and Logs** — displays the current status and activity logs of the Gateway.
- **Support** — contains a comprehensive online help system.

### Option Tabs

Each menu page may also provide sub-sections which are accessed through the use of option tabs (see [Figure 26](#) for example). To access an option, simply click on the required tab.

### Getting Help

On every screen, a *Help* button is available that provides access to the context-sensitive online help system. Click this button for further assistance and guidance relating to the current screen.

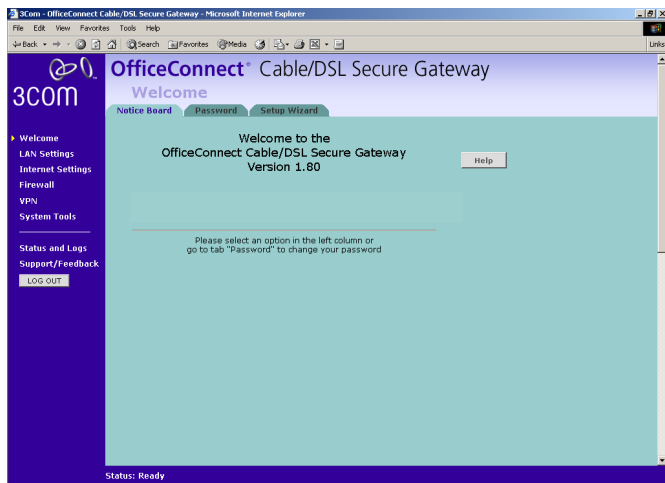
## Welcome Screen

The *Welcome* section allows you to view the Notice board and to change your Password. You can also gain access to the Configuration Wizard. See [“Accessing the Wizard”](#) on [page 23](#) for details.

## Viewing the Notice Board

The Notice Board, shown in [Figure 27](#) below, is used to display important messages. For example, you would be warned if you had disabled the Firewall or if the LAN and Internet addresses or subnets conflicted.

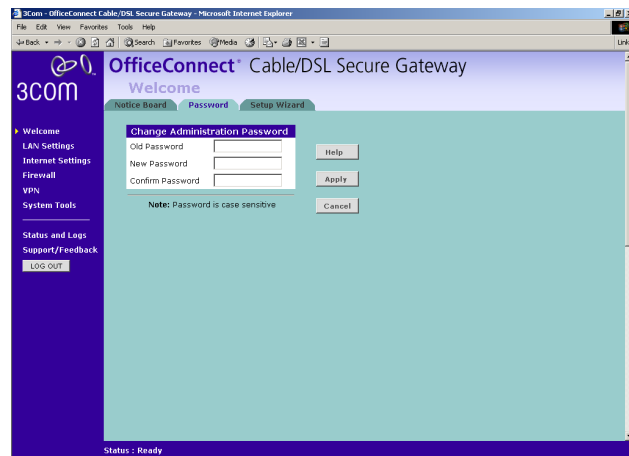
**Figure 27** Notice Board Screen



## Changing the Administration Password

You should change the password to prevent unauthorized access to the Administration System.

**Figure 28** Password Screen



To change the password:

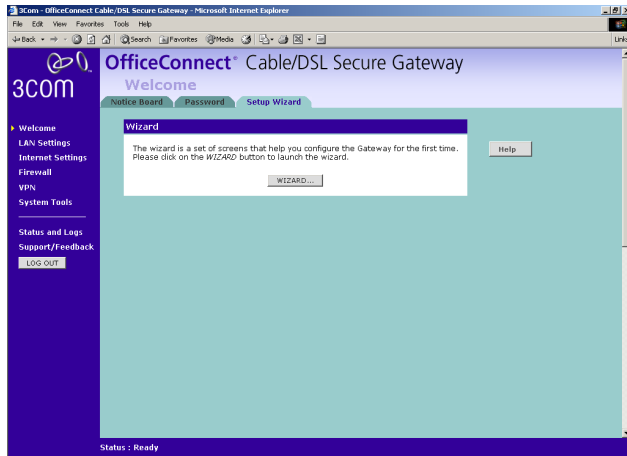
- 1 Enter the current password in the *Old Password* field.
- 2 Enter the new password in the *New Password* field.
- 3 Enter the new password again in the *Confirm Password* field.
- 4 Click *Apply* to save the new password.



*The password is case sensitive.*

## Setup Wizard

Figure 29 Wizard Screen



Click the *WIZARD...* button to launch the configuration wizard. Refer to [“Running the Setup Wizard”](#) on [page 23](#) for information on how to run the wizard.

## LAN Settings

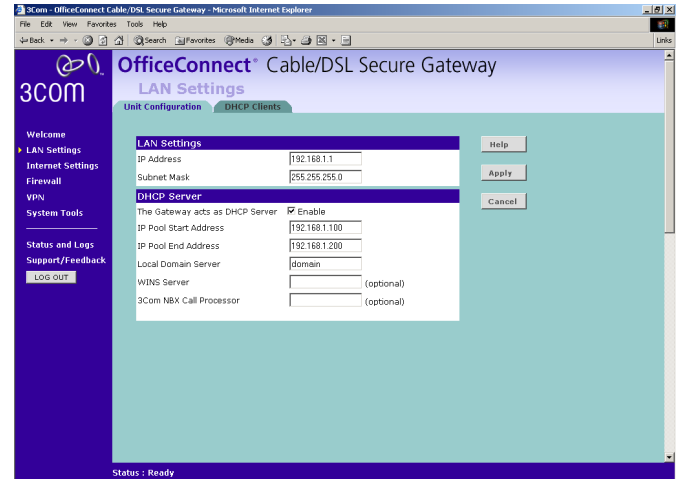
The LAN Settings menu allows you to view and amend your Gateway's:

- LAN settings.
- DHCP server settings.
- DHCP client settings.

## LAN IP Settings

The *Unit Configuration* screen allows you to change the TCP/IP settings of your Gateway and its DHCP server.


Figure 30 Unit Configuration Screen




## Changing the LAN Settings

These settings will have been entered during the set-up wizard when the device is first used. You only need to change these if you reconfigure your network. If you make any changes, click *Apply* to save them to the Gateway.


When changing the IP Address of the Gateway choose an address that will be unique in your network and in your network's subnet. The default IP Address of the Gateway is 192.168.1.1.

 When you change the IP Address of the Gateway you must reboot all computers that gain their IP address from the Gateway before they will be able to access the Internet.

 If you are using static addresses for your PCs you must alter the network configuration on each PC so that they have an IP address within the same subnet as the Gateway and have their default Gateway set as the Gateway's IP address.


If you reconfigure your network you may need to change your Subnet Mask. The Subnet Mask determines how many addresses are available to your network. The default Subnet Mask is 255.255.255.0.

For example if the IP Address of your Gateway is 192.168.1.1 and the Subnet Mask of your network is 255.255.255.0 then your network can have a maximum of 254 addresses from 192.168.1.1 to 192.168.1.254 (192.168.1.0 and 192.168.1.255 are reserved by the subnet and are not available for use).

 When you change the IP Address or Subnet Mask of the Gateway you should review the DHCP Server settings as described below.

## Changing the DHCP Server Settings

This section allows you to enable, disable and configure the settings of the Gateway's DHCP server.

 If you intend to use the Gateway to control the permissions of individual machines on your network then you must use the Gateway's DHCP server to allocate addresses (or use static addressing). If you use another DHCP server you may get unexpected results. See ["PC Privileges"](#) on [page 47](#).


To enable the DHCP Server ensure that the *Enable* check box is ticked. To disable the DHCP Server ensure that the *Enable* check box is cleared.

Set the *IP Pool Start Address* and *IP Pool End Address* to the first and last address you want the Gateway to allocate to computers. The IP address pool must be contained within the subnet as defined in ["Changing the LAN Settings"](#) on [page 35](#). The default start and end addresses are 192.168.1.100 and 192.168.1.200.

The *Local Domain Server* is set to *Domain* as default.

If you have a WINS Server on your network enter its IP address in the *WINS Server* box. The gateway will pass this information on to all Windows PCs that obtain an address from its DHCP server.

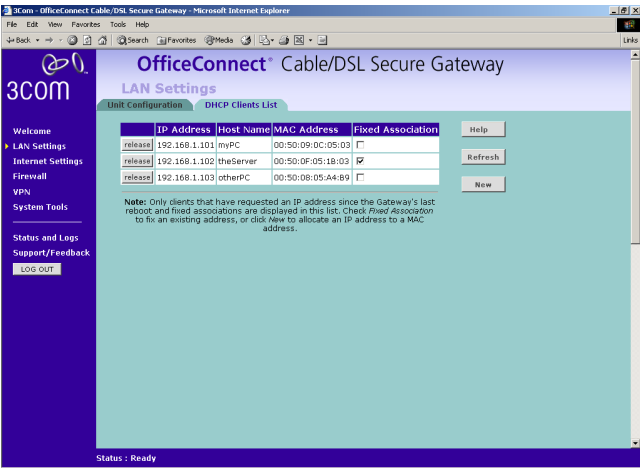
If you have a 3Com NBX Call Processor on your network enter its IP address in the *3Com NBX Call Processor* box. The 3Com NBX Call Processor acts as a switchboard for voice-over-IP phones and the gateway will pass on this information.

 If you will be using One-to-One NAT you must set up a range that is one less than the number of public addresses allocated to you by your ISP. The DHCP range must also be identical to the range specified when you set up One-to-One NAT. See ["Setting up One-to-One NAT"](#) on [page 45](#).

# DHCP Clients List

The *DHCP Clients* screen provides details of the devices that have been given IP addresses by the Gateway's DHCP server. For each device that has been granted a lease, the *IP address*, *Host Name* and *MAC address* of that device is displayed.

Figure 31 DHCP Clients Screen



The Gateway grants leases for 7 days. If a computer does not connect for a week, its IP Address may be reused.

*Expired leases are only reused when there are no free leases available. When an expired lease is re-issued the oldest lease that is not a fixed association is used.*

The *Release* button allows the lease for an IP address that has been issued to a device to be cleared. If you are running short of addresses in the DHCP Pool and you know of computers that are unlikely to connect to your network soon you can release the IP address allowing it to be reallocated to another machine.

*If you have spare or expired IP addresses in the pool you will not need to release addresses.*

The *IP Address*, *Host Name* and *MAC Address* indicate the address that has been allocated. They identify the machine by name and by the unique number (MAC Address) of the machine's network card.

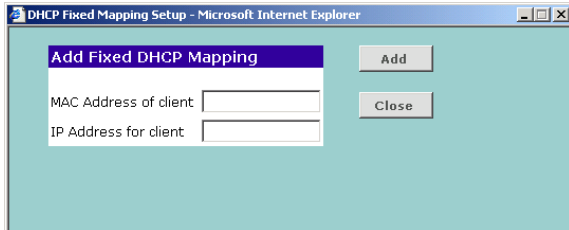
The *Fixed Association* check box allows you to freeze the relationship between an IP address and a particular machine. If you check the box for one row, that IP address will always be given out to the same machine and will not be allocated to another machine even if the lease has expired. Clear the check box to allow the address to revert back to normal behavior.

Click *Refresh* to save any changes you have made.

Click *New* to allocate an IP address to a MAC address. Click *Add* to save.

*The Gateway will attempt to supply a computer the same lease as was issued previously, even if that lease has expired.*

**Figure 32** Fixed DHCP Mapping Screen



## Internet Settings

Before you can configure the Gateway, you need to know the IP information allocation method used by your ISP. There are four different ways that ISPs can allocate IP information, as described below.



*When you install the Gateway, you will not need to use the PPPoE software on your PC.*



*When you install the Gateway, you will not need to use the dialup VPN on your PC anymore.*



*The Gateway will automatically 'dial on demand' PPPoE or PPTP and obtain data/time via NTP.*

### 1 Static IP Address (DSL or Cable)

The ISP provides the IP addressing information for you to enter manually. To configure the Gateway you will need to know the following:

- IP Address
- Subnet Mask

- ISP Gateway
- DNS address(es)

### 2 Dynamic IP Address (DSL or Cable)

Dynamic IP addressing (or DHCP) automatically assigns the Gateway IP information. This method is popular with Cable providers. This method is also used if your modem has a built in DHCP server.

### 3 PPPoE (DSL only)

If the installation instructions that accompany your modem ask you to install a PPPoE client on your PC, then select this option. To configure the Gateway you will need to know the following:

- Username
- Password
- Service Name (if required by your ISP)

### 4 PPTP (DSL or Cable)

PPTP is mainly used by some European service providers. If the installation instructions that accompany your modem ask you to setup a dialup connection using a PPTP VPN tunnel then select this option. To configure the gateway you will need to know the following:

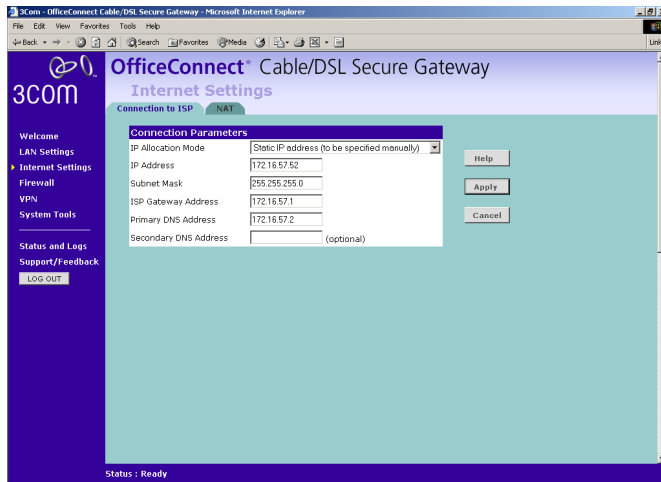
- Username
- Password
- VPN server address (usually your modem)

## Connection to ISP

This option, shown in [Figure 33](#), allows you to change the method your Gateway uses to connect to your ISP. You should only need to change these settings if:

- you change your Internet connection password (PPPoE only), or
- your ISP informs you of a change in their settings or you change ISPs.

**Figure 33** Connection to ISP Screen



Select the addressing method that your ISP uses to allocate your Gateway's Internet IP address. Choose from the options in the *IP Allocation Mode* drop-down box and the screen will refresh with options relevant to that choice.

- If you select *Static IP address (to be specified manually)* see ["Configuring a Static IP Address"](#) on [page 40](#).
- If you select *Dynamic IP address (automatically allocated)* see ["Configuring a Dynamic IP Address"](#) on [page 41](#).
- If you select *PPPoE (PPP over Ethernet)* see ["Configuring a PPPoE connection"](#) on [page 42](#).
- If you select *PPTP (used by some European providers)* see ["Configuring a PPTP connection"](#) on [page 43](#).

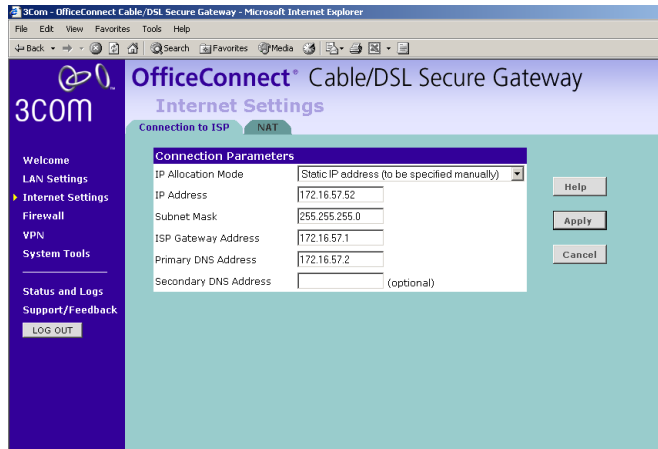


If you are using One to One NAT your method of connection will already be fixed to Static. To change to another method of address allocation you must first turn off One to One NAT. See ["Setting up NAT"](#) on [page 43](#).

## Configuring a Static IP Address

If your ISP has allocated you one or more static addresses you will have selected *Static IP address (to be specified manually)* as your *IP Allocation Mode*.

**Figure 34** Static Address Setup Screen



The screenshot shows the 'OfficeConnect Cable/DSL Secure Gateway' web interface in a Microsoft Internet Explorer browser. The 'Internet Settings' tab is active, and the 'Connection to ISP' sub-tab is selected. The 'Connection Parameters' section is displayed, showing the following fields and values:

Field	Value
IP Allocation Mode	Static IP address (to be specified manually)
IP Address	172.16.57.52
Subnet Mask	255.255.255.0
ISP Gateway Address	172.16.57.1
Primary DNS Address	172.16.57.2
Secondary DNS Address	(optional)

Buttons for 'Help', 'Apply', and 'Cancel' are located to the right of the input fields. A left-hand navigation menu includes links for Welcome, LAN Settings, Internet Settings (selected), Firewall, VPN, System Tools, Status and Logs, and Support/Feedback. A 'LOG OUT' button is at the bottom of the menu.

The following settings are required to set up Static IP address connection. Enter the values provided by your ISP:

- *IP Address* — The address allocated by your ISP for this connection.



*If you have been allocated a range of IP addresses by your ISP enter the first IP address in the range.*

- *Subnet Mask* — The subnet mask supplied by your ISP for this connection.
- *ISP Gateway Address* — The Gateway address from your ISP to the Internet.
- *Primary DNS Address* — The address of your ISP's Domain Name Service server.
- *Secondary DNS Address* — The address of your ISP's secondary Domain Name Service server. The second server is optionally provided by an ISP in case of failure of the primary server.

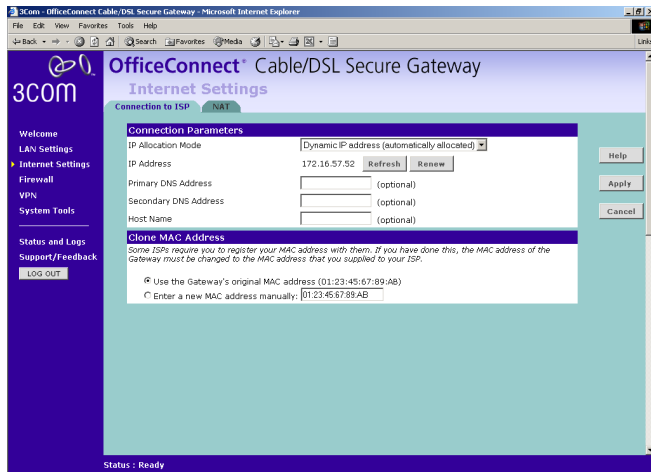
Click *Apply* to save any changes you have made.



## Configuring a Dynamic IP Address

If your ISP has allocated you a dynamic address using DHCP you will have selected *Dynamic IP address (automatically allocated)* as your *IP Allocation Mode*.

**Figure 35** Dynamic Address Setup Screen



To setup the Gateway for use with a dynamic IP address connection the following settings are configured:

- *IP Address* — The internet address allocated by your ISP for this connection is automatically configured and is not editable.

- *Subnet Mask* — The subnet for the address is automatically configured but is not displayed.
- *ISP Gateway Address* — The gateway address from your ISP to the Internet is automatically configured but is not displayed.
- *Primary DNS Address* — The address of your ISP's Domain Name Service server is automatically configured and cannot be edited.
- *Secondary DNS Address* — The address of your ISP's secondary Domain Name Service server. The second server is optionally provided by an ISP in case of failure of the primary server.
- *Host Name* — The Host Name of your computer may be required by your ISP.
- *Clone MAC Address* — Your ISP may require you to have a particular MAC address. This will be the MAC address of the computer you first used to connect with your ISP.

Click *Apply* to save any changes you have made.

## Configuring a PPPoE connection

If your ISP has allocated you a dynamic address using PPPoE you will have selected *PPPoE (PPP over Ethernet)* as your *IP Allocation Mode*.

Figure 36 PPPoE Setup Screen

The screenshot shows the 'OfficeConnect Cable/DSL Secure Gateway' interface in a Microsoft Internet Explorer browser window. The 'Internet Settings' section is expanded, and the 'Connection Parameters' tab is selected. The 'IP Allocation Mode' is set to 'PPPoE (PPP over Ethernet)'. The 'IP Address' is '172.16.57.52' with a 'Refresh' button. Other fields include 'PPPoE User Name', 'PPPoE Password', 'PPPoE Service Name' (optional), 'Primary DNS Address' (optional), 'Secondary DNS Address' (optional), 'Host Name' (optional), and 'Maximum Idle Time' set to 'forever'. 'Help', 'Apply', and 'Cancel' buttons are on the right. The status at the bottom is 'Status: Ready'.

Your ISP may need you to enter host name or PPPoE settings. To setup the Gateway for use with a PPPoE connection the following fields will need to be completed:

- *IP Address* — The internet address allocated by your ISP for this connection is automatically configured and is not editable.

- *PPPoE User Name* — The user name you use to access your ISP.
- *PPPoE Password* — The password you use to access your ISP.
- *PPPoE Service Name* — Your ISP may require you to specify a service name for your connection.
- *Primary DNS Address* — The address of your ISP's Domain Name Service server is automatically configured and is not editable.
- *Secondary DNS Address* — The address of your ISP's secondary Domain Name Service server. The second server is optionally provided by an ISP in case of failure of the primary server.
- *Host Name* — The Host Name of your computer may be required by your ISP.
- *Maximum Idle Time* — The amount of time without activity before the Gateway terminates the Internet connection.



*Since the Gateway firmware contains its own PPPoE client, you no longer need to run PPPoE client software on your computer to access the Internet. You can simply start your browser and connect to the Internet immediately after setting up your cable or DSL modem.*

## Configuring a PPTP connection

If your ISP has allocated you a dynamic address using PPTP you will have selected *PPTP (used by some European providers)* as your *IP Allocation Mode*.

Figure 37 PPTP Setup Screen

The screenshot shows the 'OfficeConnect Cable/DSL Secure Gateway' web interface. The 'Internet Settings' section is active, showing 'Connection to ISP' parameters. The 'IP Allocation Mode' is set to 'PPTP (used by some European providers)'. The 'IP Address' is 172.16.57.52. Other fields include 'PPTP Server Address', 'PPTP User Name', 'PPTP Password', 'Primary DNS Address' (optional), 'Secondary DNS Address' (optional), and 'Maximum Idle Time' (forever). A 'Help' button is present. Below this is the 'Initial IP Parameters' section with a note about specifying IP settings and a 'Suggest' button. The status at the bottom is 'Status: Ready'.

To setup the Gateway for use with a PPTP connection the following fields will need to be completed.

- *IP Address* — The internet address allocated by your ISP for this connection is automatically configured and is not editable.
- *PPTP Server Address* - This is typically the address of your modem.

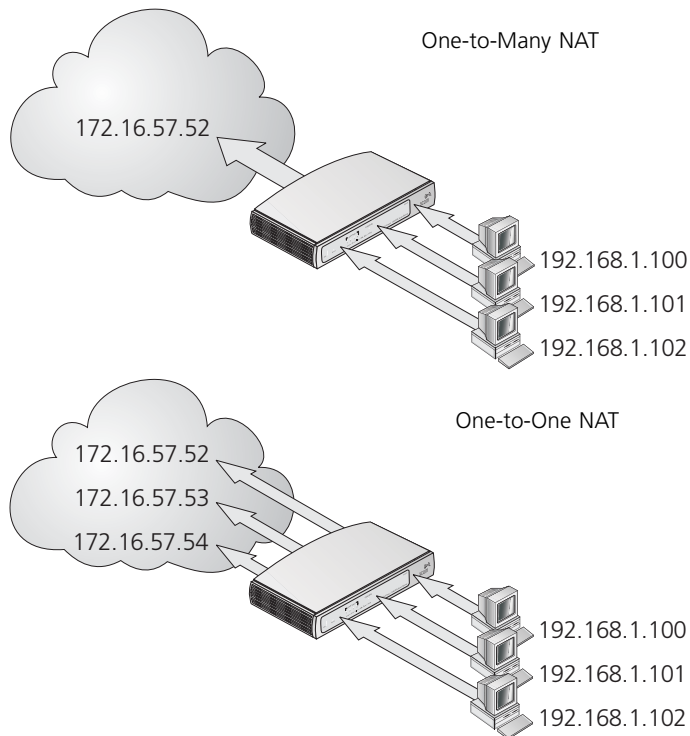
- *PPTP User Name* - The user name you use to access your ISP.
- *PPTP Password* - The password you use to access your ISP.
- *Primary DNS Address* - The address of your ISP's Domain Name Service server is automatically configured and is not editable.
- *Secondary DNS Address* - The address of your ISP's secondary Domain Name Service server. The second server is optionally provided by an ISP in case of failure of the primary server.
- *Maximum Idle Time* - The amount of time without activity before the Gateway terminates the Internet connection.
- *Initial IP Address and Initial Subnet Mask* - IP settings must be used when establishing a PPTP connection. Alternatively, if the PPTP server is located in your DSL modem, click *Suggest* to select an IP address on the same subnet as the PPTP server.

## Setting up NAT

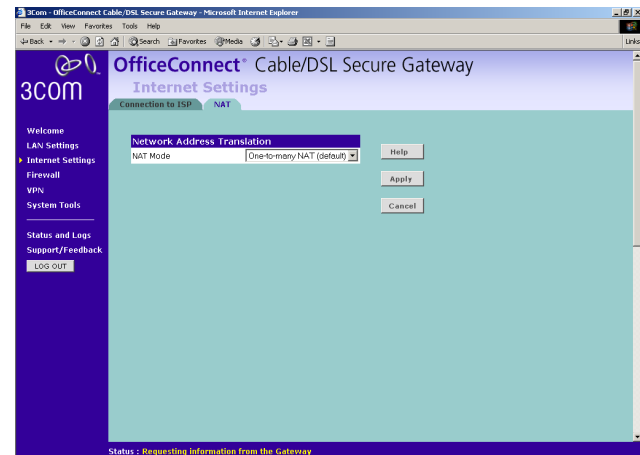
The Gateway is able to perform Network Address Translation (NAT) in one of two modes as shown in [Figure 38](#):

- *One-to-many NAT* — The Gateway shows only one address to the Internet.
- *One-to-one NAT* — Every address on the Internet pool is linked to an address in the LAN pool. The Gateway will respond to all the addresses in the Internet pool.

**Figure 38** One-to-Many and One-to-One NAT



**Figure 39** Network Address Translation Screen



### Setting up One-to-Many NAT

This is very easy to set up and the Gateway's default mode. It works with any IP Allocation Mode and will map all the addresses on your LAN to the Internet address of your Gateway. To set up One-to-Many NAT:

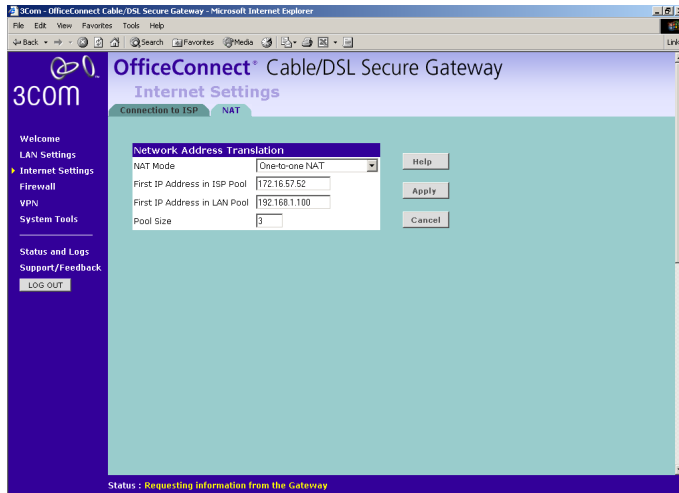
- 1 Select *One-to-Many NAT* from the *NAT Mode* drop-down box.
- 2 Click *Apply* to save your changes.

## Setting up One-to-One NAT


The following criteria must be met to be able to use One-to-One NAT:

- You must have a static Internet IP address for every computer on your network plus one for the Gateway itself.
- The addresses must be in one continuous block in the same subnet
- You must have selected *Static IP Address* as your *IP Allocation Mode* and have given your Gateway the first of the Internet addresses allocated by your ISP.

**Figure 40** One-to-One NAT Screen



To set up One-to-One NAT:

- 1 Select *One-to-One NAT* from the *NAT Mode* drop-down box.
  - 2 Enter the second address of your Internet range of addresses in the *First IP Address in ISP Pool* field.
  - 3 Enter the first address in your LAN range of addresses to which you want to map this range in the *First IP Address in LAN Pool* field.
-  *3Com recommends that you set your DHCP pool to the same as the range of LAN addresses used as your LAN pool.*
- 4 Enter the number of addresses in the range into the *Pool Size* field.
  - 5 Click *Apply* to save your changes.

---

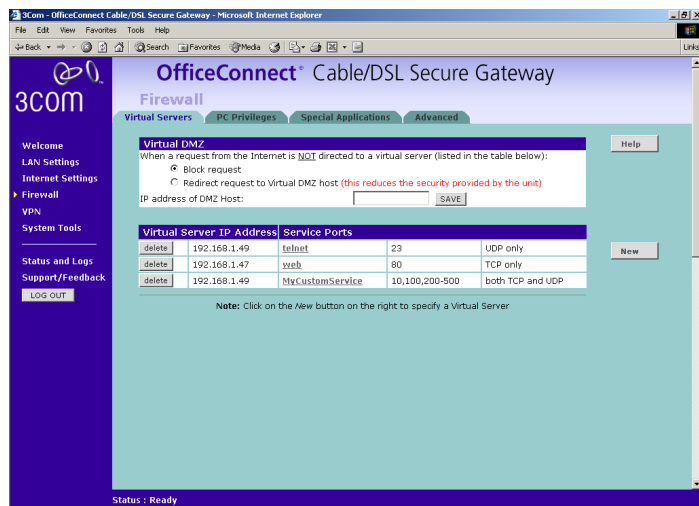
## Configuring the Firewall

On the main frame of the *Firewall* setup screen is a menu with four tabs: *Virtual Servers*, *PC Privileges*, *Special Applications*, and *Advanced*. These enable you to set the access to and security of your network.

## The Virtual Servers Menu

Selecting the *Firewall* option on the main menu displays the *Virtual Servers* screen. ([Figure 41](#))

**Figure 41** Virtual Servers Screen



## Creating a Virtual DMZ

A virtual DMZ (De-Militarized Zone) Host is a computer on your network with reduced protection provided by the firewall. This feature allows a single computer to be exposed to 2-way communication from outside of your network. The PC is still protected against DoS and hacker attacks.



**CAUTION:** This feature should be used only if the Virtual Server or Special Applications options do not provide the level of access needed for certain applications.

To configure one of your computers as a DMZ host, select *Redirect Request to Virtual DMZ Host* and enter the IP address of the computer in the *IP Address of DMZ Host* text box, and then click *SAVE*.

## Creating a Virtual Server

Activating and configuring a virtual server allows one or more of the computers on your network to function as an Internet service host. For example, one of your computers could be configured as an FTP host, allowing others outside of your office network to download files of your choosing. Or, if you have created a Web site, you can configure one of your computers as a Web server, so that others can view your Web site.

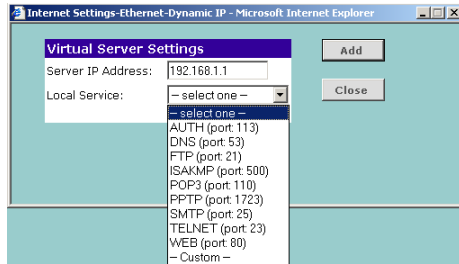


*If you are using One-to-Many NAT you can only have one server of each type on your network. To have more than one server of a type (for example more than one web server) visible to the Internet you must be using One-to-One NAT.*

To configure a virtual server:

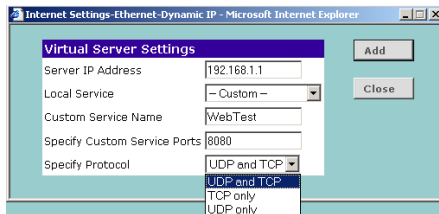
- 1 Click *New* on the right side of the screen to open the *Virtual Server Settings* dialogue box. (Figure 41)
- 2 Enter the IP address of the computer in the *Server IP Address* text box.
- 3 Select the Service from the pull-down list. (Figure 42)

**Figure 42** Virtual Servers Settings Screen



Or select *Custom* to specify a suitable name for the service and then enter the port numbers required for that service. If a service requires more than one port number enter the multiple ports as a comma separated list.

**Figure 43** Custom Setup Screen



- 4 Click *Add* to save the settings.

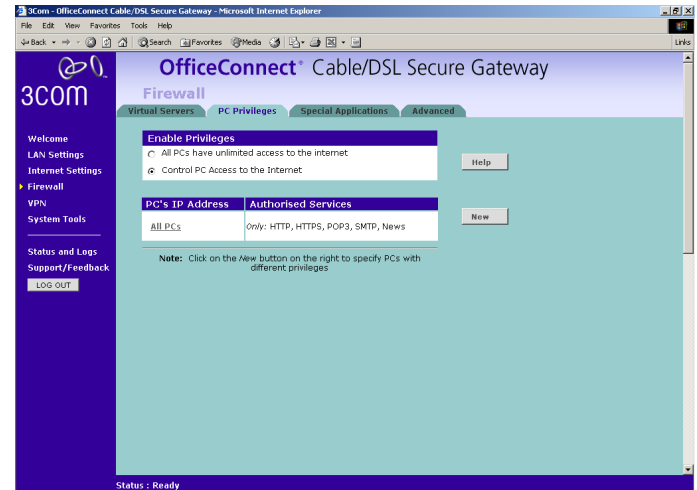
## PC Privileges

Select *PC Privileges* to display the PC Privileges setup screen. This is shown in [Figure 44](#) below.



*The Gateway's DHCP server has been enhanced to support PC Privileges. If you want to use DHCP and control access to the Internet on a user by user basis then you must either use the Gateway's DHCP server or static addressing.*

**Figure 44** PC Privileges Screen



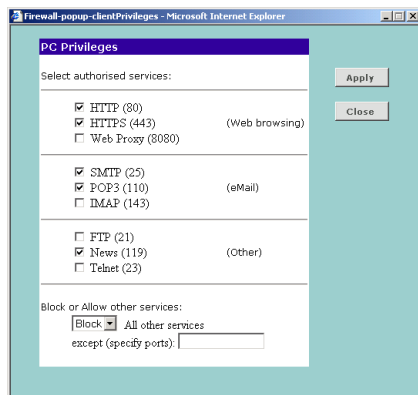
Access from the local network to the Internet can be controlled on a PC-by-PC basis. In the default configuration the Gateway will allow all connected PCs unlimited access to the Internet.

PC Privileges allows you to assign different access rights for different computers on your network, restricting this access and controlling your users' access to outside resources.

### To use access control for all computers:

- 1 Click the *Control PC Access to the Internet* radio button.
- 2 Click on *All PCs* to setup the access rights for all computers connected to the Gateway.
- 3 Check the box of a service to authorize it. Clear the box to deny the service. See [Figure 45](#).

**Figure 45** All PCs Setup Screen



- 4 Either:
  - Enter the additional services that you wish to allow in the *except (specify ports)* box and set the drop down box to *Allow*.

- Enter the services that you wish to deny in the *except (specify ports)* box and set the drop down box to *Deny*.



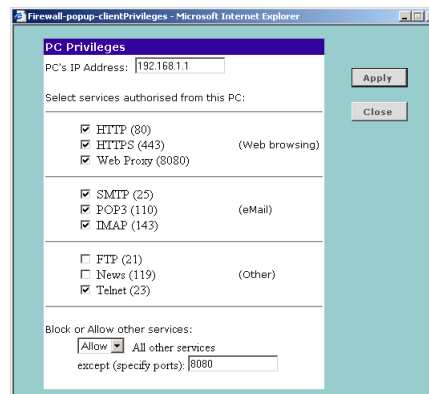
Enter multiple ports as either a comma separated list e.g. 101, 105, 107, or as a range, e.g. 101-107.

- 5 Click *Apply* to save the settings.

### To assign different access rights for different computers:

- 1 Click the *Control PC Access to the Internet* radio button.
- 2 Click *New* to display the *PC Privileges* setting screen.
- 3 Enter the IP address of the computer in the *PC's IP Address* text box.
- 4 Check the box of a service to authorize it. Clear the box to deny the service. See [Figure 46](#).

**Figure 46** PC Privileges Setup Screen





5 Either:

- Enter the additional services that you wish to allow in the *except (specify ports)* box and set the drop down box to *Allow*.
- Enter the services that you wish to deny in the *except (specify ports)* box and set the drop down box to *Deny*.



Enter multiple ports as either a comma separated list e.g. 101, 105, 107, or as a range, e.g. 101-107.

6 Click *Apply* to save the settings.

**Example:** Allowing only web and E-mail access.

To allow web and E-mail access and block all other services across the Gateway's firewall:

- Ensure that the *Control PC Access to the Internet* radio button is selected.
- Click on *All PCs* to pop up the *PC Privileges* window.
- Ensure that the *Email (110,25)* and *Web (80)* boxes are checked and that other check-boxes are left cleared.
- Set the *Block or Allow other services:* drop-down box to *Block* other services.

For the purposes of this example, your users also need to access a test web server on port 8080. To allow this:

- Enter the number *8080* in the *except (specify ports):* box.
- Click *Apply* to save your changes and close the *PC Privileges* window.

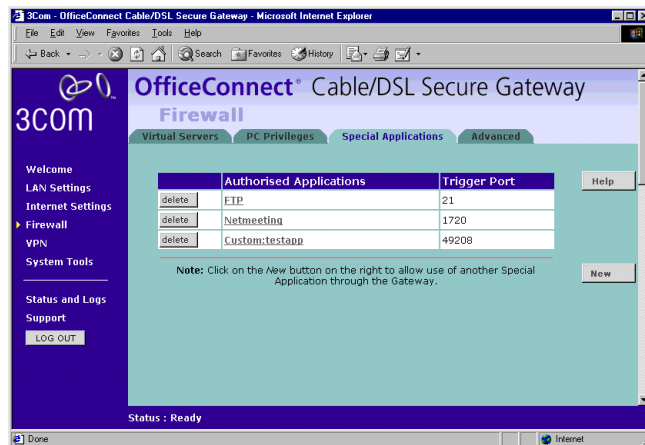


VPN connections to other networks are unaffected by settings in *PC Privileges*. To allow or deny VPN connections to other networks see [“Configuring VPNs”](#) on [page 53](#).

## Special Applications

Select *Special Applications* tab to display the *Authorized Application* setup screen. See [Figure 47](#) below.

**Figure 47** Special Applications Screen



Some software applications need a connection to be started from the Internet — an act that is usually blocked by the Gateway's firewall.

So that these special applications can work properly and are not blocked, the firewall needs to be told about them. In each instance there will be an outgoing trigger which tells the Gateway's firewall that the application has started and to allow the incoming connections.



*Each defined Special Application only supports a single computer user and any incoming ports opened by a Special Application trigger will be closed after 20 minutes of inactivity for TCP/IP connections or 10 for UDP/IP connections.*

For each special application configured by the Gateway, a row is added to the table. Each row contains the following items:

- **Delete** button — Deletes the special application on that row. This will prevent the Gateway's firewall from opening to that connection.
- **Name** — Each special application is named. This name is not used by the Gateway and is only to enable you to identify the connection. Clicking the name of a connection displays the *Special Application Setup* screen. See [“Adding and Editing Special Applications”](#) below.
- **Trigger Port** — This is the TCP/IP port number that the Gateway uses to recognize that the application has started.

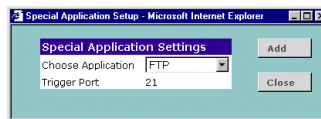
Additionally there are two buttons outside the table:

- **Help** — displays the online help page for this screen.
- **New** — creates a new special application. See [“Adding and Editing Special Applications”](#) below.

## Adding and Editing Special Applications

- 1 Click on the **New** button to create a new special application or on the name of a special application to edit the settings for that application.

**Figure 48** Special Application Settings Screen



- 2 Select the applications from the *Choose Application* drop-down box. See [Figure 48](#). If the application you want to define is not in the list select *Custom* and see [“Creating Custom Special Applications”](#) below.
- 3 Click **Add** to add the special application to the list of protocols or **Close** to abort your selection and return to the *Special Applications* screen.

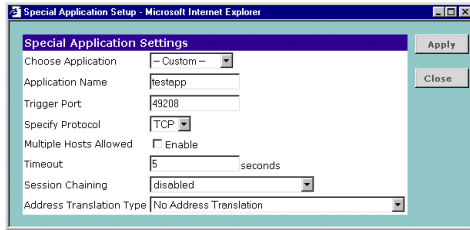


*Depending on the settings you have made in PC Privileges the Special Application you have defined may not be allowed across the Firewall. See [“PC Privileges”](#) on [page 47](#).*

## Creating Custom Special Applications

If your special application is not listed in the *Choose Application* drop-down box you can still configure it manually. Select *Custom* from the *Choose Application* drop-down box and the Special Application Setup Screen gains the extra fields needed to describe a custom special application. These are shown in [Figure 49](#) below.

**Figure 49** Custom Special Applications Setup Screen



- **Application Name** — Each special application is named and will detect the ports that need to be opened so you do not need to specify them. This name is not used by the Gateway and is only to enable you to identify the connection.
- **Trigger Port** — This is the TCP/IP port number that the Gateway uses to recognize the outgoing packet that starts special application session. Your application provider can provide you with this information.



*The Gateway allows Trigger Ports that are a single value or a range of values but not a list. So '6599' and '6577-6587' are both valid but '6577, 6579, 6582' is not.*

- **Specify Protocol** — Select the protocol (TCP or UDP) that your special application uses. Your application provider can provide you with this information.
- **Multiple Hosts Allowed** — If your application provider uses more than one IP address during a session or responds from an address different to the one you use to start the special application then you must ensure that the *Multiple Hosts Allowed* box is checked. Otherwise leave it clear. Your application provider can provide you with this information.



**CAUTION:** *Selecting Multiple Hosts Allowed weakens the security that your Gateway's firewall is able to provide and should only be used if the special application requires it.*

- **Timeout** — Enter the number of seconds the Gateway should wait for the first reply from the special application server before it abandons the connection.



*The default Timeout is three seconds. If you find that connections are being dropped enter a higher value.*

- **Session Chaining** — Some special applications need to take control of a session. If the special application you wish to run requires this ensure that *Session Chaining* is enabled otherwise ensure that it is disabled.



**CAUTION:** *Allowing Session Chaining weakens the security that your Gateway's firewall is able to provide and should only be used if the special application requires it.*

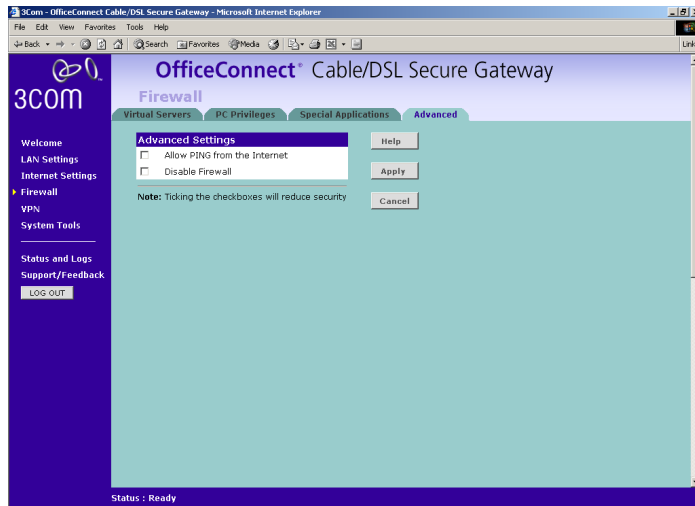
- **Address Translation Type** — If your special application provider embeds IP addresses in TCP or UDP packets you will have to enable address translation on the appropriate protocol type. Your application provider can provide you with this information.

When you have configured your special application click *Add* to save your changes or *Close* to quit without making any changes.

## Advanced

Select *Advanced* to display the Advanced Settings screen. See [Figure 50](#) below.

**Figure 50** Advanced Settings Screen



The Internet connects millions of computer users throughout the world. The vast majority of the computer users on the Internet are friendly and have no intention of breaking into, stealing from, or damaging your network. However, there are hackers who may try to break into your network.

The options on this screen enable you to allow PING from the internet and to disable the firewall as shown below:

- *Allow PING from the Internet* — PING is a utility, which is used to determine whether a device is active at the specified IP address. PING is normally used to test the physical connection between two devices, to ensure that everything is working correctly.

By default the Gateway has PING disabled so that it does not respond to PING requests. This makes the device more difficult to find on the Internet and less prone to attack.

This feature is enabled by clicking on the check box so that a tick can be seen and then selecting *Apply*.



*3Com recommends that you leave Allow PING from the Internet disabled as this provides greater security.*

- *Disable Firewall* — The Gateway contains a firewall that detects attack patterns used by hackers on the Internet and once detected will block their access to your network. The Firewall is disabled by clicking on the check box so that a tick can be seen and then clicking *Apply*.




*3Com recommends that you leave the firewall enabled (checkbox cleared) for normal use. You may wish to turn it off for diagnostic purposes.*

---

## Configuring VPNs

A Virtual Private Network (VPN) is a secure tunnel between networks or between a network and a user. The Gateway supports both network to network connections and network to remote client connections.

The Gateway supports IPSec tunnels, L2TP over IPSec, and PPTP connections and allows VPN pass-through to enable other secure devices on your network to set up their own secure connections.

 *Your Cable/DSL modem and your ISP must support IPSec pass-through, L2TP over IPSec pass-through or PPTP pass-through for you to be able to use these protocols.*


See [“The Virtual Servers Menu”](#) on [page 45](#) for details to configure pass-through protocols.


## Setting the VPN Mode

The Gateway supports three modes of VPN operation:

- **IPSec Enabled** — IPSec (Internet Protocol Security) is a complex secure protocol with a variety of different encryption methods. When setting up an IPSec connection between two devices they must support the same encryption method.
- **L2TP over IPSec Enabled** — L2TP over IPSec is a combination of protocols which authenticates a user (using L2TP) and encrypts data (using IPSec). See [“L2TP Configuration”](#) on [page 54](#).

- **PPTP Server Enabled** — PPTP (Point-to-Point Tunnelling Protocol) is an encrypted VPN protocol like IPSec. It is not as secure as IPSec but is easy to administrate. PPTP does not support Gateway to Gateway connections and is only suitable for connecting remote users.


 *Enabling IPSec VPN will disable pass-through to IPSec and L2TP/IPSec Virtual Servers on the LAN. Enabling L2TP over IPSec will disable pass-through to IPSec and L2TP/IPSec Virtual Servers on the LAN. Enabling the PPTP server will disable PPTP pass-through to a Virtual Server on the LAN. Pass-through outbound from clients on the LAN to servers on the internet is unaffected.*

 *A VPN Tunnel needs the same protocol on both sides of the connection. If you are trying to establish an IPSec connection with another Gateway or with a user the other Gateway must support IPSec or the user must have software installed that supports IPSec VPN.*

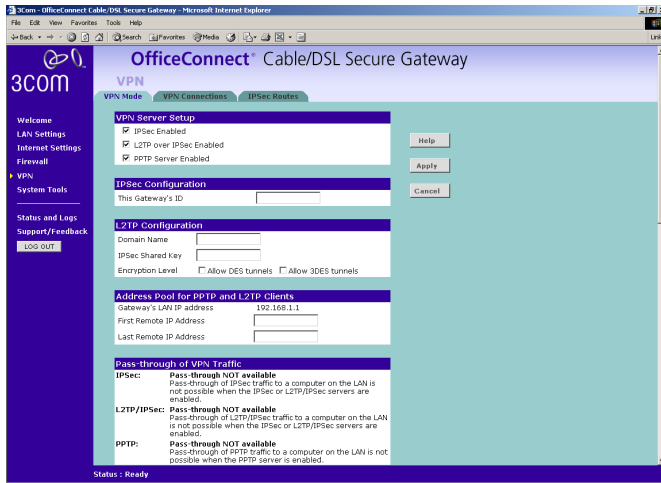
The VPN Mode menu is shown in [Figure 51](#) below. Choose from the options by clicking in the appropriate radio button under *VPN Server Setup*.

### IPSec Configuration

In the *IPSec Configuration* field, enter *This Gateway's ID* as an Internet IP address or name of the Gateway that you are configuring. This value is common across all IPSec connections but does not apply to PPTP connections. If PPTP only is enabled, *This Gateway's ID* field does not appear.

 *If you require main mode IPSec connections then this value must be the public IP address of the Gateway.*

**Figure 51** VPN Mode Screen



## L2TP Configuration

If you have enabled L2TP over IPsec you must enter the following items:

- 1 In the *IPsec Configuration* field, enter *This Gateway's ID* as an Internet IP address or name of the Gateway that you are configuring. This value is common across all IPsec connections but does not apply to PPTP connections. If PPTP only is enabled, *This Gateway's ID* field disappears.
- 2 In the *L2TP Configuration* field, enter:
  - the *Domain Name* as an IP address. A Domain Name locates a website on the Internet.

- The *IPsec Shared Key*. This is the key for the connection and is a combination of letters, numbers and punctuation and can be up to 64 characters in length. 3Com recommends that the key and password are not the same. The user will need to know the IPsec Shared Key to enable connection.
- In the *Encryption Level* field, choose either *Allow DES tunnels* or *Allow 3DES tunnels*. 3DES is more secure but may take longer to encrypt and decrypt.



*3DES is not shipped with the Gateway as standard due to international restrictions on encryption. If your country permits its use it can be downloaded from the 3Com web site at <http://www.3com.com/>*

- 3 To set up the Gateway for L2TP over IPsec you must allocate IP addresses from the Gateway's LAN for use with L2TP over IPsec. The connections made by L2TP over IPsec will appear to come from these addresses. The addresses must be in a continuous range.

In the *Address Pool for PPTP and L2TP clients* field enter:

- The first LAN address you wish to reserve for L2TP over IPsec in the *First Remote IP Address* field.
- The last LAN address you wish to reserve for L2TP over IPsec in the *Last Remote IP Address* field.

If PPTP mode is selected, then the Address Pool is the same for PPTP and L2TP over IPsec clients.



*These addresses must be within the Gateway's LAN subnet and must not form part of the DHCP pool..*

- 4 Click *Apply* to save your changes.

## PPTP Configuration

To set up the Gateway for PPTP you must allocate IP addresses from the Gateway's LAN for use with PPTP. The connections made by PPTP will appear to come from these addresses. The addresses must be in a continuous range.

In the *Address Pool for PPTP and L2TP clients* field enter:

- The first LAN address you wish to reserve for PPTP clients in the *First Remote IP Address* field.
- and
- The last LAN address you wish to reserve for PPTP clients in the *Last Remote IP Address* field.

If L2TP mode is selected, then the Address Pool is the same for PPTP and L2TP over IPSec clients.



*These addresses must be within the Gateway's LAN subnet and must not form part of the DHCP pool.*

Click *Apply* to save your changes.

## Viewing VPN Connections

The VPN Connections Screen shows information about the IPSec, L2TP over IPSec, and PPTP connections made by the Gateway. It also allows you to add, delete, edit and temporarily disable these connections.

**Figure 52** VPN Connections Screen

OfficeConnect Cable/DSL Secure Gateway				
VPN				
VPN Mode    VPN Connections    IPSec Routes				
<b>IPSec Connections with Other Servers</b>				
<a href="#">delete</a>	Hemel	Tunnel to main office ACTIVE: 4512770 bytes tunnelled	IPSec	<input checked="" type="checkbox"/>
<b>Connections from Remote Users</b>				
<a href="#">delete</a>	disabled user	An IPSec client user DISABLED	IPSec	<input type="checkbox"/>
<a href="#">delete</a>	Robt.L2TP	Tunnel for Win98 road warrior ACTIVE: 17955 bytes tunnelled	L2TP/ IPSec	<input checked="" type="checkbox"/>
<a href="#">delete</a>	Remote	Tunnel for road warrior NOT ACTIVE	IPSec	<input checked="" type="checkbox"/>
<a href="#">delete</a>	userRobt	Tunnel for Win98 road warrior ACTIVE: 1270 bytes tunnelled	PPTP	<input checked="" type="checkbox"/>

Note: Click on the New button to add a new connection.

Status: Ready

For each connection configured for the Gateway, a row is added to the table. Each row contains the following items:

- *Delete* button — deletes the VPN connection on that row. This will prevent the device or user from establishing a secure connection with the Gateway in future.

- **Name** — Identifies the tunnel. Clicking the name of a connection displays the *Edit VPN Connection* screen. See [“Adding and Editing VPN Connections”](#) below.
- **Description** — A text description that enables you to identify a connection. This field in the table additionally displays whether the connection is currently active.
- **Type** — Indicates the type of connection.
- **Enabled** — This check box allows you to enable or disable a connection without deleting it and thus losing the connection details. Check this box to enable a connection. Clear this box to disable the connection. If the connection is active it will be disconnected.

Additionally there are three buttons outside the table:

- **Help** — displays the online help page for this screen.
- **Refresh** — updates the contents of the window allowing you to see the current status of connections.
- **New** — creates a new VPN connection. See [“Adding and Editing VPN Connections”](#) below.

## Adding and Editing VPN Connections

This screen allows you to add new IPSec, L2TP over IPSec and PPTP connections and to edit existing ones. When adding or amending values on this screen remember that both sides of an IPSec, L2TP over IPSec or PPTP connection must contain the same information.

An IPSec, L2TP over IPSec or PPTP connection cannot therefore be activated until both ends of the tunnel have been configured.

- **Connection Name/User Name** — the ID of the remote gateway (the value entered in *This Gateway's ID* on the remote gateway or the remote user's login name). This can be a name (containing numbers and letters but no punctuation) or an IP address but cannot be a domain name.



*If the Connection Name is set using numeric IP addresses then the Gateway to Gateway connection will use main mode. Otherwise it will use aggressive mode.*

- **Description** — a description of the connection. This can be different on each Gateway as it is not used in the connection.
- **Connection Type** — choose either *Gateway to Gateway* (only available with IPSec) to connect to another Gateway or *Remote User Access* to create a connection for a remote computer.



*If the remote site has another gateway with an established IPSec, L2TP over IPSec or PPTP connection then there is no need to create a connection for a remote user on that site.*



*If you configure an IPSec connection for a remote computer then that computer will require software that supports IPSec. If you configure an L2TP over IPSec or PPTP connection for a remote computer then you should contact Microsoft for information on whether an upgrade is required.*

- **Tunnel Type** — Choose either IPSec (either Remote User Access or Gateway to Gateway), L2TP over IPSec or PPTP.



Depending on which Tunnel Type you have selected, choose from the following to edit or add the remaining fields:

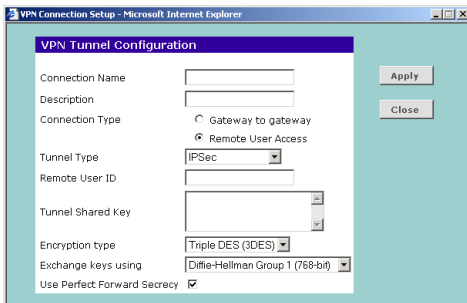
- ["IPSec Connections using Remote User Access"](#) on [page 57](#)
- ["IPSec Connections using Gateway to Gateway"](#) on [page 57](#)
- ["L2TP over IPSec Connections"](#) on [page 59](#)
- ["PPTP Connections"](#) on [page 60](#)

### IPSec Connections using Remote User Access

If you have selected IPSec as a Tunnel Type and Remote User Access as a Connection Type, enter the following values:

- **Remote User ID** — Enter the Remote User ID. This must be entered identically on the IPSec software installed on the client's machine.
- **Tunnel Shared Key** — this is the password for the connection and is a combination of letters, numbers and punctuation and can be up to 64 characters in length.

**Figure 53** IPSec Connection - Remote User Access



- **Encryption type** — choose the encryption type from DES or 3DES. 3DES is more secure but may take longer to encrypt and decrypt.



*3DES is not shipped with the Gateway as standard due to international restrictions on encryption. If your country permits its use it can be downloaded from the 3Com web site at*

**<http://www.3com.com/>**

- **Exchange keys using** — choose the encryption method used to exchange shared keys. *Diffie-Hellman Group 2* is more secure but less common than *Diffie-Hellman Group 1*.
- **Use Perfect Forward Secrecy** — Choose whether to use perfect forward secrecy. Using perfect forward secrecy will change the encryption keys during the course of a connection making the tunnel more secure but slowing data transfer. To enable perfect forward secrecy ensure that the *Use Perfect Forward Secrecy* box is checked. To keep the same key for the length of a connection leave the box unchecked.

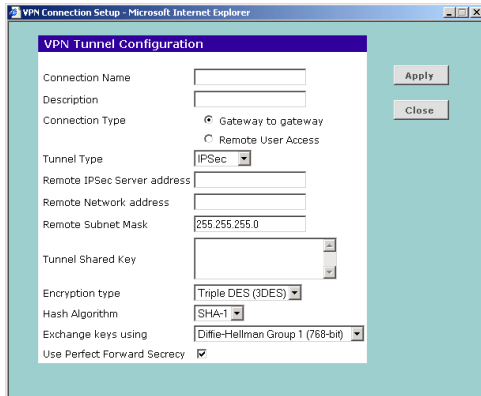
Click *Apply* to save your changes or *Close* to return without saving.

### IPSec Connections using Gateway to Gateway

If you have selected IPSec as a Tunnel Type and Gateway to Gateway as a Connection Type, enter the following values:

- **Remote IPSec Server Address** — enter the Internet IP address or name of the remote gateway. ([Figure 54](#)).
- **Remote Network address** — enter the LAN IP address of the remote network. This is the first IP address of a subnet, one below the first address available for use.

**Figure 54** IPSec Connection - Gateway to Gateway



*If the remote Gateway has a LAN IP address of 192.168.1.1 and a subnet mask of 255.255.255.0 then the LAN IP address of the remote subnet is 192.168.1.0.*



*The Gateways must be configured with LAN IP address ranges that do not overlap.*

- **Remote Subnet address** — this is set as 255.255.255.0 as default.
- **Tunnel Shared Key** — this is the password for the connection and is a combination of letters, numbers and punctuation and can be up to 64 characters in length.



*If you are creating a Gateway to Gateway connection you have no need to remember the Tunnel Shared Key once the tunnel is established and do not have to make the key a memorable password.*

- **Encryption type** — choose the encryption type from DES or 3DES. 3DES is more secure but may take longer to encrypt and decrypt.



*3DES is not shipped with the Gateway as standard due to international restrictions on encryption. If your country permits its use it can be downloaded from the 3Com web site at <http://www.3com.com/>*

- **Hash Algorithm** — choose either SHA-1 or MD5 from the drop-down list. Both ends of the connection must use the same value.
- **Exchange keys using** — choose the encryption method used to exchange shared keys. *Diffie-Hellman Group 2* is more secure but less common than *Diffie-Hellman Group 1*.
- **Use Perfect Forward Secrecy** — Choose whether to use perfect forward secrecy. Using perfect forward secrecy will change the encryption keys during the course of a connection making the tunnel more secure but slowing data transfer. To enable perfect forward secrecy ensure that the *Use Perfect Forward Secrecy* box is checked. To keep the same key for the length of a connection leave the box unchecked.

**Example:** Setting up an IPSec connection between two Gateways.

Gateway One is located at the head office and is configured with the following settings:

- Internet IP address: 172.27.34.202
- LAN IP address: 192.168.1.1
- LAN Subnet Mask: 255.255.255.0

Gateway Two is located at the sales office and is configured with the following settings:

- Internet IP address: 174.27.34.202
- LAN IP address: 192.168.2.1
- Remote Subnet Mask: 255.255.255.0

To set up an IPSec Connection between the two Gateways, do the following on each Gateway:

- 1 Select *IPSec Enabled* from the *VPN Mode* screen.
- 2 Switch to the *VPN Connections* screen and click *New*.
- 3 In the *Connection Name* field enter: *headsales*
- 4 In the *Description* field enter: *Connection between head office and sales office.*
- 5 Ensure that the *Gateway to gateway* radio button is selected.
- 6 Enter the Internet IP address of the Gateway you are configuring in the *This Gateway's ID* field.
  - a Enter 174.19.201.162 on Gateway One.
  - b Enter 172.27.34.202 on Gateway Two.
- 7 Enter the Internet IP address of the other Gateway in the *Remote IPSec Server Address* field.
  - a Enter 174.27.34.202 on Gateway One.
  - b Enter 172.19.201.162 on Gateway Two.
- 8 Enter the IP address of the other LAN subnet in the *Remote Network address* field.
  - a Enter 192.168.2.0 on Gateway One.
  - b Enter 192.168.1.0 on Gateway Two.

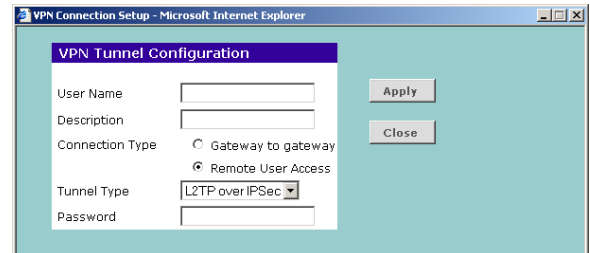
- 9 The *Remote Subnet Mask* is a default setting of 255.255.255.0.
- 10 Enter a password in the *Tunnel Shared Key* field in both Gateways. The example uses *TYP0249//23b* as the shared key.
- 11 Choose *DES* as the *Encryption Type*.
- 12 Choose SHA-1 as the *Hash Algorithm*.
- 13 Choose Diffie-Hellman Group 1 (768 bit) the in the *Exchange keys using* drop-down box.
- 14 Ensure that the *Use Perfect Forward Secrecy* box is checked
- 15 Click *Apply* to save your changes or *Close* to return without saving.

## L2TP over IPSec Connections

If you have selected L2TP over IPSec as your Tunnel Type, enter the following values. See [Figure 55](#):

- *Password* — The password that will need to be supplied to connect.

**Figure 55** L2TP over IPSec Connections



Click *Apply* to save your changes or *Close* to return without saving. When you have created a user account the user will need to know in order to enable connection.

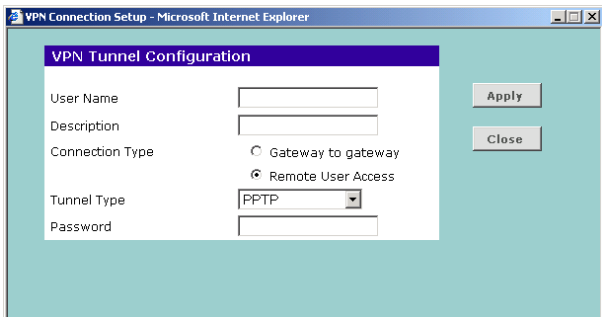
## PPTP Connections

If you have selected PPTP as a Tunnel Type, enter the following:

- *Password* — The Password that the user will need to supply to connect. (Figure 56)

When you have created a user account the user will need to know the User Name and Password you have given them.

**Figure 56** PPTP Connections



The screens to edit and add a PPTP user contain the same fields.

Click *Apply* to save your changes or *Close* to return without saving.

## Editing IPsec Routes

This screen allows you to add and replace networks in the existing IPsec Route. See [Figure 57](#)

To do this:

- 1 Select *edit* to display the *Edit Route* screen. ([Figure 58](#)).
- 2 Click in the table and add a new *Network* and *Subnet Mask* entry.
- 3 Click *Apply* to save your changes or *Close* to return without saving.



*The gateway for a remote network must also be set to use the VPN tunnel to access your local network. Therefore, if you include a subnet for a remote network in your IPsec route then the remote network must also include your subnet in its IPsec route also.*

Figure 57 IPsec Routes

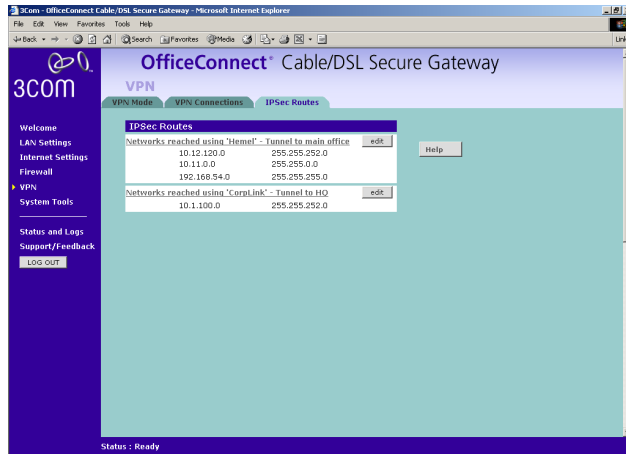
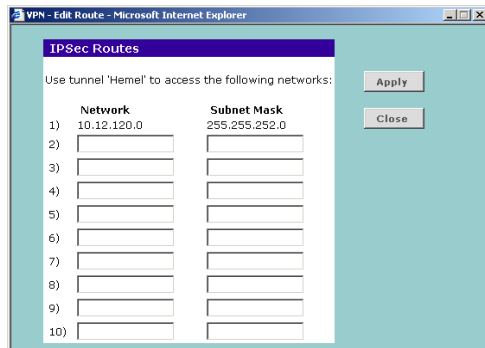


Figure 58 Edit Route



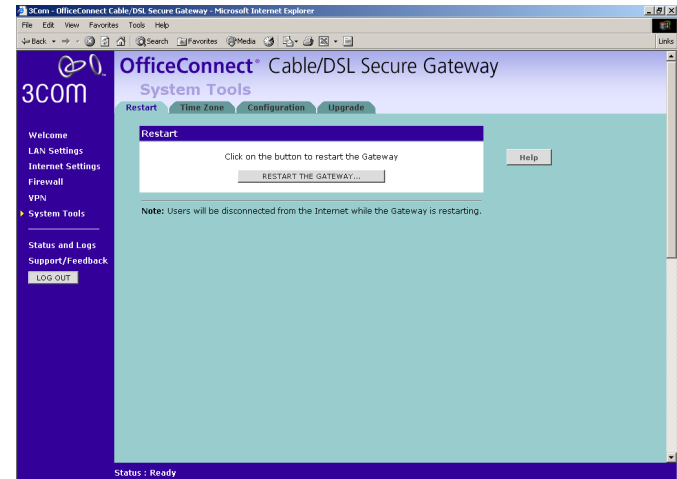
## Accessing the System Tools

The System Tools menu includes four administration items: *Restart*, *Time Zone*, *Configuration*, and *Upgrade*. See [Figure 59](#).

## Restart

Pressing the *Restart the Gateway* button has the same effect as power cycling the unit. No configuration information will be lost but the log files will be erased. This function may be of use if you are experiencing problems and you wish to re-establish your Internet connection.

Figure 59 Restart Screen



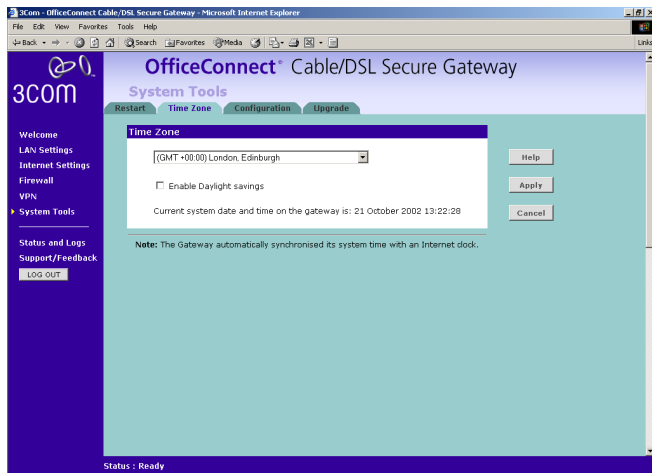
Any network users who are currently accessing the Internet will have their access interrupted whilst the restart takes place, and they may need to reboot their computers when the restart has completed and the Gateway is operational again.

## Time Zone

Choose the time zone that is closest to your actual location. The time zone setting is used by the system clock when displaying the correct time in the log files.

If you use Daylight saving tick the Enable Daylight savings box, and then click *Apply*. ([Figure 60](#))

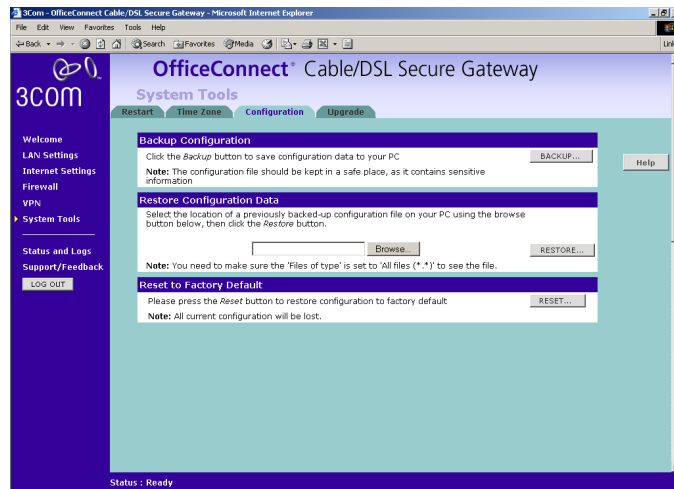
**Figure 60** Time Zone Screen



The Gateway reads the correct time from NTP servers on the Internet and sets its system clock accordingly. The Daylight Savings option automatically adjusts the clock to daylight savings time as appropriate to your time zone.

## Loading and Saving the Gateway Configuration

**Figure 61** Configuration Screen



Select the *Configuration* tab to display the *Configuration* screen ([Figure 61](#)).

- Click *BACKUP* to save the current configurations of the OfficeConnect Cable/DSL Secure Gateway. You will be prompted to download and save a file to disk.

- If you want to reinstate the configuration settings previously saved to a file, click *Browse* to locate the backup file on your computer, and then *RESTORE* to copy the configuration back to the Gateway.



*For security purposes restoring the configuration does not change the password.*

- If you want to reset the settings on your Gateway to those that were loaded at the factory, click *RESET*. You will lose all your configuration changes. The Gateway LAN IP address will revert to 192.168.1.1, and the DHCP server on the LAN will be enabled. You may need to reconfigure and restart your computer to re-establish communication with the Gateway.

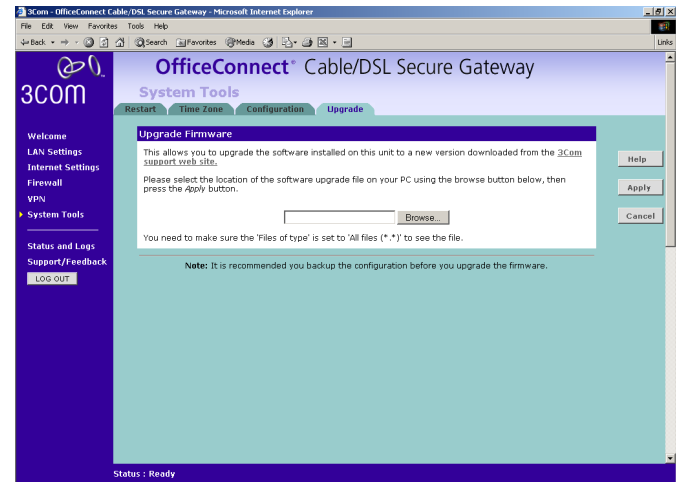
## Upgrading the Firmware of your Gateway

The Upgrade facility allows you to install on the Gateway any new releases of system software that 3Com may make available.



*3DES encryption is not shipped with the Gateway as standard due to international restrictions on encryption. If your country permits its use it can be downloaded from the 3Com web site at <http://www.3com.com/>*

**Figure 62** Upgrade Screen



Once you have downloaded the software, use the *Browse* button to locate the file on your computer, and then click on *Apply*.



*You may need to change the file type in the dialog box displayed by your web browser to \*.\* to be able to see the file.*

The file will be copied to the Gateway, and once this has completed, the Gateway will restart. Although the upgrade process has been designed to preserve your configuration settings, 3Com recommends that you make a backup of the configuration beforehand, in case the upgrade process fails for any reason (for example, the connection between the computer and the Gateway is lost while the new software is being copied to the Gateway).

The upgrade procedure can take a few minutes, and is complete when the Alert LED has stopped flashing and is permanently off. Make sure that you do not interrupt power to the Gateway during the upgrade procedure; if you do, the software may be corrupted and the Gateway may not start up properly afterwards. If the Alert LED comes on continuously or flashing slowly after a failed upgrade, refer to [“Troubleshooting”](#) on [page 67](#).

## Viewing Status and Logs

Selecting *Status and Logs* from the Main menu displays the *Status* and *Logs* screens in your Web browser. The *Status* and *Logs* screen displays a tabular representation of your network and Internet connection.

*Status* — to display the current unit status, including a summary of the configuration. See [Figure 63](#).

*Log Settings* — to choose whether to store the log on the Gateway or to send to the remote user or both. See [Figure 64](#).



*If you choose the option to store the log on the Gateway the log file will be overwritten when it is full. If you choose the option to send logs to a remote server then you will need to specify the IP address of the remote server. The IP address must be within the LAN subnet and a syslog server must be installed on the remote server.*

*Logs* — to view both the normal events, and security threats logged by the Gateway

**Figure 63** Status Screen

The screenshot shows the 'OfficeConnect Cable/DSL Secure Gateway' web interface. The 'Status' tab is selected, displaying a summary of the gateway's configuration and current status. The interface includes a sidebar menu with options like Welcome, LAN Settings, Internet Settings, Firewall, VPN, System Tools, Status and Logs (selected), and Support/Feedback. The main content area is divided into several sections:

- General Information:** Software version (1.00), Hardware version (01.00), 3C number (3C856-95), and Serial Number (7X9V601BD30).
- Access From the Internet:** Network Address Translation (One-to-many NAT (default)), Firewall Switched On (YES), Discard PING from the internet side (YES), and VPN Tunnels Open (0).
- Internet Settings:** PPP over Ethernet Enabled (NO), Internet IP Address (172.16.57.52), Internet Subnet Mask (255.255.255.0), DNS (172.16.57.10, 172.16.57.1), Remaining Lease Time (00:18:01), and Internet MAC Address (00:05:1A:61:BD:31).
- LAN Settings:** LAN IP Address (192.168.1.1), LAN Subnet Mask (255.255.255.0), LAN MAC Address (00:03:1A:81:CD:43), and Gateway's DHCP Server (ENABLED).
- Hardware Status:** Internet Port Status (10 Mbps, Half-Duplex), LAN Port #1 Status (100 Mbps, Full-Duplex), and LAN Port #2 Status (No Link).

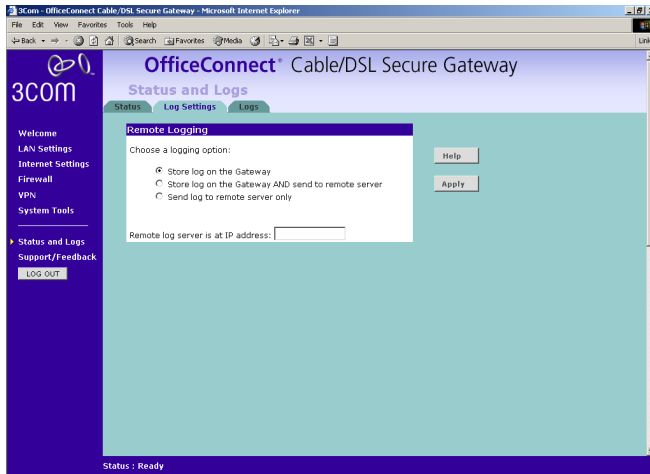
Buttons for 'Help' and 'Refresh' are located on the right side of the General Information section. The status at the bottom of the page is 'Status : Ready'.



*You may be asked to refer to the information on the Status screen if you contact your supplier for technical support.*



**Figure 64** Log Settings Screen

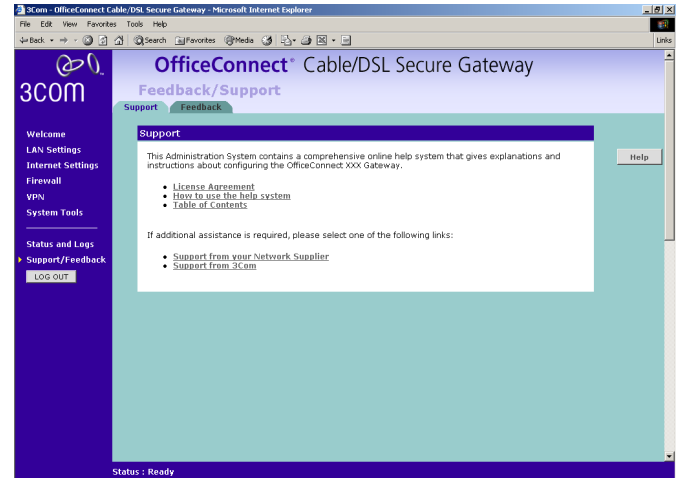


## Obtaining Support and Feedback for your Gateway

Selecting *Support/Feedback* on the main menu generates both:

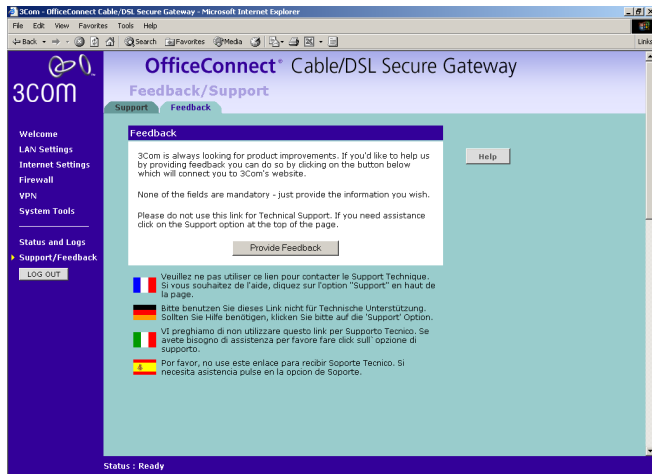
- The support links screen, which contains a list of Internet links that provide information and support concerning the Gateway. (Figure 65)

**Figure 65** Support Screen



- The feedback links screen, which contains an Internet link to the 3Com website so that you can provide feedback on the product. (Figure 66)

Figure 66 Feedback Screen



# TROUBLESHOOTING

---

## Basic Connection Checks

- Check that the Gateway is connected to your computers and to the Cable/DSL modem, and that all the equipment is powered on. Check that the LAN and Cable/DSL port link status LEDs on the Gateway are illuminated, and that any corresponding LEDs on the Cable/DSL modem and the NIC are also illuminated.
- Ensure that the computers have completed their start-up procedure and are ready for use. Some network interfaces may not be correctly initialized until the start-up procedure has completed.
- If the link status LED does not illuminate for a port that is connected, check that you do not have a faulty cable. Try a different cable.

---

## Browsing to the Gateway Configuration Screens

If you have connected your Gateway and computers together but cannot browse to the Gateway configuration screens, check the following:

- Confirm that the physical connection between your computer and the Gateway is OK, and that the link status LEDs on the Gateway and NIC are illuminated and indicating the same speed (10Mbps or 100Mbps). Some NICs do not have status LEDs, in which case a diagnostic program may be available that can give you this information. Refer to the documentation supplied with your NIC for details.

- Ensure that you have configured your computer as described in [“Setting Up Your Computers”](#) on [page 19](#). Restart your computer while it is connected to the Gateway to ensure that your computer receives an IP address.
- When entering the address of the Gateway into your web browser, ensure that you include the full URL including the `http://` prefix. (e.g. **http://192.168.1.1**)
- If you cannot browse to the Gateway, use the *winipcfg* utility in Windows 95/98/ME to verify that your computer has received the correct address information from the Gateway. From the *Start* menu, choose *Run* and then enter **winipcfg**. Check that the computer has an IP address of the form 192.168.1.xxx (where xxx is in the range 2-254), the subnet mask is 255.255.255.0, and the default Gateway is 192.168.1.1 (the address of the Gateway). If these are not correct, use the *Release* and *Renew* functions to obtain a new IP address from the Gateway. Under Windows NT/2000/XP, use the *ipconfig* command-line utility to perform the same functions.
- If you still cannot browse to the Gateway, then use the Discovery program on the accompanying CD-ROM as described in [“Using Discovery”](#) on [page 71](#).

---

## Connecting to the Internet

If you can browse to the Gateway configuration screens but cannot access sites on the Internet, check the following:

- Confirm that the physical connection between the Gateway and the Cable/DSL modem is OK, and that the link status LEDs on both Gateway and modem are illuminated.
- Confirm that the connection between the modem and the Cable/DSL interface is OK.
- Ensure that you have entered the correct information into the Gateway configuration screens as required by your Internet Service Provider. Use the "Internet Settings" screen to verify this.
- For DSL users, check that the PPPoE or PPTP user name, password and service name are correct, if these are required. Only enter a PPPoE service name if your ISP requires one.
- For cable users, check whether your ISP requires a fixed MAC (Ethernet) address. If so, use the *Clone MAC Address* feature in the Gateway to ensure that the correct MAC address is presented, as described in ["Configuring a Dynamic IP Address"](#) on [page 41](#).
- Ensure that your computers are not configured to use a Web proxy. On Windows computers, this can be found under *Control Panel > Internet Options > Connections*.
- Check PC Privileges to see if you have allowed your PCs to connect to the Internet. See ["PC Privileges"](#) on [page 47](#).

---

## Forgotten Password

If you can browse to the Gateway configuration screen but cannot log on because you do not know or have forgotten the password, follow the steps below to reset the Gateway to its factory default configuration. **Warning: all your configuration changes will be lost, and you will need to run the configuration wizard again before you can re-establish your Gateway connection to the Internet.** Also, other computer users will lose their network connections whilst this process is taking place, so choose a time when this would be convenient.

- 1 Remove power from the Gateway.
- 2 Disconnect all your computers and the cable/DSL modem from the Gateway.
- 3 Using an Ethernet cable, connect the Ethernet Cable/DSL port on the rear of the Gateway to any one of the LAN ports.
- 4 Re-apply power to the Gateway. The Alert LED will flash as the Gateway starts up, and after approximately 30 seconds will start to flash more slowly (typically 2 seconds on, 2 seconds off). Once the Alert LED has started to flash slowly, remove power from the Gateway.
- 5 Remove the cable connecting the Cable/DSL port to the LAN port, and reconnect one of your computers to one of the Gateway LAN ports.

- 6 Re-apply power to the Gateway, and when the start-up sequence has completed, browse to:

**http://192.168.1.1**

and run the configuration wizard. You may need to restart your computer before you attempt this.

- 7 When the configuration wizard has completed, you may reconnect your network as it was before.

---

## Alert LED

The Alert LED will flash when the Gateway unit is first powered up while the system software checks the hardware for proper operation. Once the Gateway has started normal operation, the Alert LED will go out.

- If the Alert LED does not go out following start up, but illuminates continuously, this indicates that the software has detected a possible fault with the hardware. If the Alert LED is flashing slowly this indicates a firmware failure. Remove power from the Gateway, wait 10 seconds and then re-apply power. If the Alert LED comes on continuously again, then a fault has been detected. Locate the copy of the Gateway software on the accompanying CD-ROM and upload it to the Gateway to see if this clears the fault (refer to “Recovering from Corrupted Software” below). If this does not fix the problem, contact your supplier for further advice.
- During normal operation, you may notice the Alert LED lighting briefly from time to time. This indicates that the Gateway has detected a hacker attack from the Internet and has prevented it from harming your network. You need take no specific action on this, unless you decide that these attacks

are happening frequently in which case you may wish to discuss this with your ISP. The Gateway logs such attacks, and this information is available through the configuration screens.

---

## Recovering from Corrupted Software

If the Alert LED remains permanently on following power-up, it is possible that the system software has become corrupted. In this condition, the Gateway will enter a failsafe state; DHCP is disabled, and the LAN IP address is set to 192.168.1.1. Follow the instructions below to upload a new copy of the system software to a Gateway unit in this state.

Ensure that one of your computers has a copy of the new software image file stored on its hard disk or available on CD-ROM.

- 1 Remove power from the Gateway and disconnect the Cable/DSL modem and all your computers, except for the one computer with the software image.
- 2 You will need to reconfigure this computer with the following static IP address information:
  - IP address: 192.168.1.2
  - Subnet mask: 255.255.255.0
  - Default Gateway address: 192.168.1.1
- 3 Restart the computer, and re-apply power to the Gateway.
- 4 Using the Web browser on the computer, enter the following URL in the location bar:

**http://192.168.1.1**

This will connect you to the failsafe mode of the Gateway.

- 5 Follow the on-screen instructions. Enter the path and filename of the software image file.
- 6 When the upload has completed, the Gateway will restart, run the self-test and, if successful, resume normal operation. The Alert LED will go out.
- 7 Refer to the Installation Guide to reconnect your Gateway to the Cable/DSL modem and the computers in your network. Do not forget to reconfigure the computer you used for the software upload.

If the Gateway does not resume normal operation following the upload, it may be faulty. Contact your supplier for advice.

---

## Frequently Asked Questions

### **How many computers on the LAN does the Cable/DSL Secure Gateway support?**

A maximum of 253 computers on the LAN are supported.

### **There are only 4 LAN ports on the Gateway. How are additional computers connected?**

You can expand the number of connections available on your LAN by using hubs and switches connected to the Gateway. 3Com OfficeConnect hubs and switches provide a simple, reliable means of expanding your network; contact your supplier for more information, or visit:

<http://www.3com.com>

### **Does the Gateway support virtual private networks (VPNs)?**

The Gateway fully supports VPNs. It is capable of:

- Initiating and terminating IPSec connections.
- Terminating L2TP over IPSec and PPTP connections.
- Providing hardware accelerated encryption for IPSec VPNs and IPSec VPNs within L2TP over IPSec.
- Providing VPN pass-through.

### **Where can I download software upgrades for the Gateway?**

Upgrades to the Cable/DSL Secure Gateway software are posted on the 3Com support web site, accessible by visiting:

<http://www.3com.com>

### **What other online resources are there?**

The 3Com Knowledgebase at:

<http://knowledgebase.3com.com>

is a database of technical information covering all 3Com products. It is updated daily with information from 3Com technical support services, and it is available 24 hours a day, 7 days a week.


# USING DISCOVERY

## Running the Discovery Application

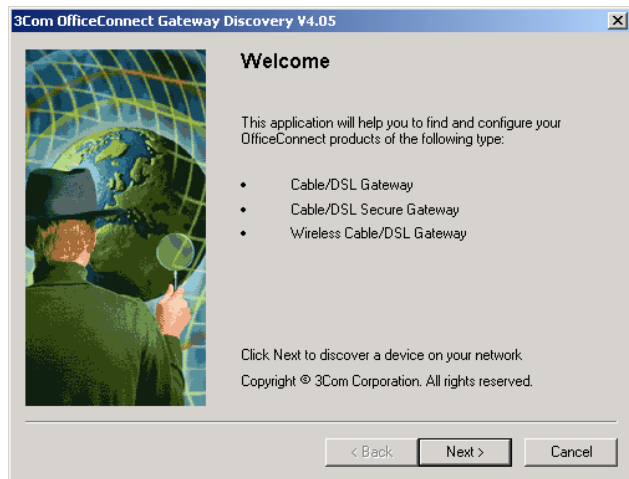
3Com provides a user-friendly Discovery application for detecting the OfficeConnect Cable/DSL Secure Gateway on the network.

## Windows Installation (95/98/2000/Me/NT)

- 1 Insert the Gateway CD-ROM in the CD-ROM drive on your computer. A menu will appear; select *Gateway Discovery*.

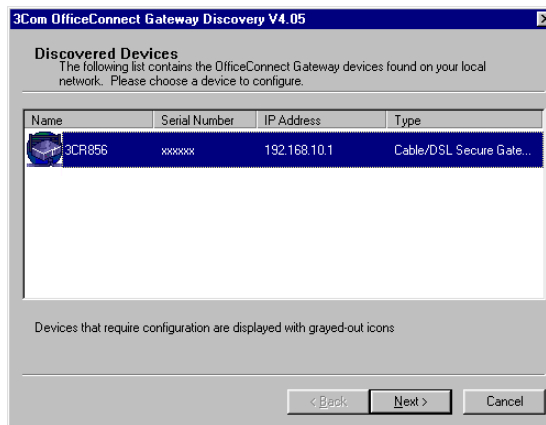
 *Discovery will find the Gateway even if it is unconfigured or misconfigured.*

**Figure 67** Discovery Welcome Screen



- 2 When the *Welcome* screen is displayed click on *Next* and wait until the application discovers the Gateways connected to your LAN.

**Figure 68** Discovered Gateway



*In [Figure 68](#) the serial number of the unit has been replaced with xxxxxx.*

- 3 [Figure 68](#) shows an example Discovered Devices screen. Highlight the Cable/DSL Secure Gateway by clicking on it, and press *Next*.

**Figure 69** Discovery Finish Screen



- 4 Click on *Finish* to launch a web browser and display the login page for the Gateway.



# IP ADDRESSING

## The Internet Protocol Suite

The Internet protocol suite consists of a well-defined set of communications protocols and several standard application protocols. Transmission Control Protocol/Internet Protocol (TCP/IP) is probably the most widely known and is a combination of two of the protocols (IP and TCP) working together. TCP/IP is an internationally adopted and supported networking standard that provides connectivity between equipment from many vendors over a wide variety of networking technologies.

## IP Addresses and Subnet Masks

Each device on your network must have a unique IP address to operate correctly. An IP address identifies the address of the device to which data is being sent and the address of the destination network. IP addresses have the format n.n.n.x where n is a decimal number between 0 and 255 and x is a number between 1 and 254 inclusive.

However, an IP Address alone is not enough to make your device operate. In addition to the IP address, you need to set a subnet mask. All networks are divided into smaller sub-networks and a subnet mask is a number that enables a device to identify the sub-network to which it is connected.

For your network to work correctly, all devices on the network must have:

- The same sub-network address.
- The same subnet mask.



*The only value that will be different is the specific host device number. This value must always be unique.*

An example IP address is '192.168.100.8'. However, the size of the network determines the structure of this IP Address. In using the Gateway, you will probably only encounter two types of IP Address and subnet mask structures.

### Type One

In a small network, the IP address of '192.168.100.8' is split into two parts:

- Part one ('192.168.100') identifies the network on which the device resides.
- Part two ('.8') identifies the device within the network.

This type of IP Address operates on a subnet mask of '255.255.255.0'.

See [Table 3](#) for an example about how a network with three PCs and a Cable/DSL Secure Gateway might be configured.

**Table 3** IP Addressing and Subnet Masking in a Small Network

Device	IP Address	Subnet Mask
PC 1	192.168.100.8	255.255.255.0
PC 2	192.168.100.33	255.255.255.0
PC 3	192.168.100.188	255.255.255.0
Cable/DSL Secure Gateway	192.168.100.72	255.255.255.0

## Type Two

In larger networks, where there are more devices, the IP address of '192.168.100.8' is, again, split into two parts but is structured differently:

- Part one ('192.168') identifies the network on which the device resides.
- Part two ('.100.8') identifies the device within the network.

This type of IP Address operates on a subnet mask of '255.255.0.0'.

See [Table 4](#) for an example about how a network (only four PCs represented) and a Cable/DSL Secure Gateway might be configured.

**Table 4** IP Addressing and Subnet Masking in a Large Network

Device	IP Address	Subnet Mask
PC 1	192.168.100.8	255.255.0.0
PC 2	192.168.201.30	255.255.0.0
PC 3	192.168.113.155	255.255.0.0
PC 4	192.168.2.230	255.255.0.0
Cable/DSL Secure Gateway	192.168.2.72	255.255.0.0

---

## How does a Device Obtain an IP Address and Subnet Mask?

There are three different ways to obtain an IP address and the subnet mask. These are:

- Dynamic Host Configuration Protocol (DHCP) Addressing
- Static Addressing
- Automatic Addressing (Auto-IP Addressing)

### DHCP Addressing

The Cable/DSL Secure Gateway contains a DHCP server, which allows computers on your network to obtain an IP address and subnet mask automatically. DHCP assigns a temporary IP address and subnet mask which gets reallocated once you disconnect from the network.

DHCP will work on any client Operating System such as Windows® 95, Windows 98 or Windows NT 4.0. Also, using DHCP means that the same IP address and subnet mask will never be duplicated for devices on the network. DHCP is particularly useful for networks with large numbers of users on them.

### Static Addressing

You must enter an IP Address and the subnet mask manually on every device. Using a static IP and subnet mask means the address is permanently fixed.

## Auto-IP Addressing

Network devices use automatic IP addressing if they are configured to acquire an address using DHCP but are unable to contact a DHCP server. Automatic IP addressing is a scheme where devices allocate themselves an IP address at random from the industry standard subnet of 169.254.x.x (with a subnet mask of 255.255.0.0). If two devices allocate themselves the same address, the conflict is detected and one of the devices allocates itself a new address.

Automatic IP addressing support was introduced by Microsoft in the Windows 98 operating system and is also supported in Windows 2000.

---

## Private IP Addresses

The following address ranges have been reserved by the Internet Engineering Task Force (IETF) for private use:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

The Gateway has a default subnet of 192.168.1.0 – 192.168.1.255. 3Com recommends that you use this subnet for the LAN addresses of your first Gateway and subsequent ranges (192.168.2.0 – 192.168.2.255) for the LAN range of other Gateways that you will connect to by VPN.



# TECHNICAL SPECIFICATIONS

This section lists the technical specifications for the OfficeConnect Cable/DSL Secure Gateway.

## Interfaces

Cable or DSL modem connection - one 10/100 Mbps Ethernet port (10BASE-T/100BASE-TX) with auto-MDIX.

LAN connection - four 10/100 Mbps Ethernet ports (10BASE-T/100BASE-TX) with auto-MDIX.

## Operating Temperature

0 °C to 40 °C (32 °F to 105 °F)

## Power

7 W power dissipated

## Humidity

0 % to 90 % (non-condensing) humidity

## Dimensions

Width = 220 mm (8.7 in.)

Depth = 135 mm (5.3 in.)

Height = 36 mm (1.4 in.)

## Weight

Approximately 537 g (1.18 lbs)

---

## Standards

Functional:ISO 8802/3  
IEEE 802.3

Safety:UL 60950, EN 60950  
CSA 22.2 #60950  
IEC 60950

EMC:EN 55022 Class B<sup>†</sup>  
EN 55024  
AS/NZS 3548 B<sup>†</sup>  
FCC Part 15 Class B<sup>†\*</sup>  
ICES-003 Class B<sup>†</sup>  
VCCI Class B<sup>†</sup>  
CNS 13438 Class A

Environmental:EN 60068 (IEC 68)

<sup>†</sup>Category 5 screened cables must be used to ensure compliance with the Class B requirements of this standard. The use of unscreened cables (Category 3 or Category 5) complies with the Class A requirements.



*Category 5 cables must be used if you are connecting to 100 Mbps devices.*

\*See [“Safety Information” on page 79](#) for conditions of operation.

---

## System Requirements

### Operating Systems

The Cable/DSL Secure Gateway will support the following Operating Systems:

- Windows 95, 98, Me
- Windows NT 4.0
- Windows 2000
- Windows XP
- Mac OS 8.5 or higher
- Unix

---

### Ethernet Performance

The Cable/DSL Secure Gateway complies to the IEEE 802.3i, u and x specifications.

---

### Cable Specifications

The Cable/DSL Secure Gateway supports the following cable types and maximum lengths:

- Category 3 (Ethernet) or Category 5 (Fast Ethernet or Dual Speed Ethernet) Twisted Pair — shielded and unshielded cable types.
- Maximum cable length of 100m (327.86 ft).



*Category 5 cables are required for a 100BASE-TX connection.*

# SAFETY INFORMATION

---

## Important Safety Information



**WARNING:** Warnings contain directions that you must follow for your personal safety. Follow all directions carefully.

You must read the following safety information carefully before you install or remove the unit:



**WARNING:** Exceptional care must be taken during installation and removal of the unit.



**WARNING:** Only stack the Gateway with other OfficeConnect units.



**WARNING:** To ensure compliance with international safety standards, only use the power adapter that is supplied with the unit.



**WARNING:** The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.



**WARNING:** This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 60950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.



**WARNING:** There are no user-replaceable fuses or user-serviceable parts inside the Gateway. If you have a physical problem with the unit that cannot be solved with

problem solving actions in this guide, contact your supplier.



**WARNING:** Disconnect the power adapter before moving the unit.



**WARNING: RJ-45 ports.** These are shielded RJ-45 data sockets. They cannot be used as telephone sockets. Only connect RJ-45 data connectors to these sockets.

---

## Wichtige Sicherheitshinweise



**VORSICHT:** Warnhinweise enthalten Anweisungen, die Sie zu Ihrer eigenen Sicherheit befolgen müssen. Alle Anweisungen sind sorgfältig zu befolgen. Sie müssen die folgenden Sicherheitsinformationen sorgfältig durchlesen, bevor Sie das Gerät installieren oder ausbauen:



**VORSICHT:** Bei der Installation und beim Ausbau des Geräts ist mit höchster Vorsicht vorzugehen.



**VORSICHT:** Stapeln Sie das Gerät nur mit anderen OfficeConnect Geräten zusammen.



**VORSICHT:** Aufgrund von internationalen Sicherheitsnormen darf das Gerät nur mit dem mitgelieferten Netzadapter verwendet werden.



**VORSICHT:** Die Netzsteckdose muß in der Nähe des Geräts und leicht zugänglich sein. Die Stromversorgung des Geräts kann nur durch Herausziehen des Gerätenetzkabels aus der Netzsteckdose unterbrochen werden.



**VORSICHT:** Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 60950. Diese Bedingungen sind nur gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden.



**VORSICHT:** Es sind keine von dem Benutzer zu ersetzende oder zu wartende Teile in dem Gerät vorhanden. Wenn Sie ein Problem mit dem Gateway haben, das nicht mittels der Fehleranalyse in dieser Anleitung behoben werden kann, setzen Sie sich mit Ihrem Lieferanten in Verbindung.



**VORSICHT:** Vor dem Ausbau des Geräts das Netzadapterkabel herausziehen.



**VORSICHT: RJ-45-Anschlüsse.** Dies sind abgeschirmte RJ-45-Datenbuchsen. Sie können nicht als Telefonanschlußbuchsen verwendet werden. An diesen Buchsen dürfen nur RJ-45-Datenstecker angeschlossen werden.

---

## Consignes importantes de sécurité



**AVERTISSEMENT:** Les avertissements présentent des consignes que vous devez respecter pour garantir votre sécurité personnelle. Vous devez respecter attentivement toutes les consignes.  
Nous vous demandons de lire attentivement les consignes suivantes de sécurité avant d'installer ou de retirer l'appareil:



**AVERTISSEMENT:** Faites très attention lors de l'installation et de la dépose du groupe.



**AVERTISSEMENT:** Seulement entasser le moyeur avec les autres moyeux OfficeConnects.



**AVERTISSEMENT:** Pour garantir le respect des normes internationales de sécurité, utilisez uniquement l'adaptateur électrique remis avec cet appareil.



**AVERTISSEMENT:** La prise secteur doit se trouver à proximité de l'appareil et son accès doit être facile. Vous ne pouvez mettre l'appareil hors circuit qu'en débranchant son cordon électrique au niveau de cette prise.



**AVERTISSEMENT:** L'appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme CEI 60950. Ces conditions ne sont maintenues que



*si l'équipement auquel il est raccordé fonctionne dans les mêmes conditions.*



**AVERTISSEMENT:** *Il n'y a pas de parties remplaçables par les utilisateurs ou entretenues par les utilisateurs à l'intérieur du moyeu. Si vous avez un problème physique avec le moyeu qui ne peut pas être résolu avec les actions de la résolution des problèmes dans ce guide, contacter votre fournisseur.*



**AVERTISSEMENT:** *Débranchez l'adaptateur électrique avant de retirer cet appareil.*



**AVERTISSEMENT: Ports RJ-45.** *Il s'agit de prises femelles blindées de données RJ-45. Vous ne pouvez pas les utiliser comme prise de téléphone. Branchez uniquement des connecteurs de données RJ-45 sur ces prises femelles.*



# END USER SOFTWARE LICENCE AGREEMENT

## 3Com Corporation END USER SOFTWARE LICENSE AGREEMENT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE DOWNLOADING, INSTALLING AND USING THIS PRODUCT, THE USE OF WHICH IS LICENSED BY 3COM CORPORATION ("3COM") TO ITS CUSTOMERS FOR THEIR USE ONLY AS SET FORTH BELOW. DOWNLOADING, INSTALLING OR OTHERWISE USING ANY PART OF THE SOFTWARE OR DOCUMENTATION INDICATES THAT YOU ACCEPT THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL OR OTHERWISE USE THE SOFTWARE OR DOCUMENTATION, DO NOT CLICK ON THE "I AGREE" OR SIMILAR BUTTON. AND IF YOU HAVE RECEIVED THE SOFTWARE AND DOCUMENTATION ON PHYSICAL MEDIA, RETURN THE ENTIRE PRODUCT WITH THE SOFTWARE AND DOCUMENTATION UNUSED TO THE SUPPLIER WHERE YOU OBTAINED IT.

**LICENSE:** 3Com grants you a nonexclusive, nontransferable (except as specified herein) license to use the accompanying software program(s) in executable form (the "Software") and accompanying documentation (the "Documentation"), subject to the terms and restrictions set forth in this Agreement. You are not permitted to lease, rent, distribute or sublicense (except as specified herein) the Software or Documentation or to use the Software or Documentation in a time-sharing arrangement or in any other unauthorized manner. Further, no license is granted to you in the human readable code of the Software (source code). Except as provided below, this Agreement does not grant you any rights to patents, copyrights, trade secrets, trademarks, or any other rights with respect to the Software or Documentation.

Subject to the restrictions set forth herein, the Software is licensed to be used on any workstation or any network server owned by or leased to you, for your internal use, provided that the Software is used only in connection with this 3Com product. You may reproduce and provide one (1) copy of the Software and Documentation for each such workstation or network server on which the Software is used as permitted hereunder. Otherwise, the Software and Documentation may be copied only as essential for backup or archive purposes in support of your use of the Software as permitted hereunder. Each copy of the Software and Documentation must contain 3Com's and its licensors' proprietary rights and copyright notices in the same form as on the original. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation delivered to you under this Agreement.

**ASSIGNMENT; NO REVERSE ENGINEERING:** You may transfer the Software, Documentation and the licenses granted herein to another party in the same country in which you obtained the Software and Documentation if the other party agrees in writing to accept and be bound by the terms and conditions of this Agreement. If you transfer the Software and Documentation, you must at the same time either transfer all copies of the

Software and Documentation to the party or you must destroy any copies not transferred. Except as set forth above, you may not assign or transfer your rights under this Agreement.

Modification, reverse engineering, reverse compiling, or disassembly of the Software is expressly prohibited. However, if you are a European Union ("EU") resident, information necessary to achieve interoperability of the Software with other programs within the meaning of the EU Directive on the Legal Protection of Computer Programs is available to you from 3Com upon written request.

**EXPORT RESTRICTIONS:** The Software, including the Documentation and all related technical data (and any copies thereof) (collectively "Technical Data"), is subject to United States Export control laws and may be subject to export or import regulations in other countries. In addition, the Technical Data covered by this Agreement may contain data encryption code which is unlawful to export or transfer from the United States or country where you legally obtained it without an approved U.S. Department of Commerce export license and appropriate foreign export or import license, as required. You agree that you will not export or re-export the Technical Data (or any copies thereof) or any products utilizing the Technical Data in violation of any applicable laws or regulations of the United States or the country where you legally obtained it. You are responsible for obtaining any licenses to export, re-export or import the Technical Data.

In addition to the above, the Product may not be used, exported or re-exported (i) into or to a national or resident of any country to which the U.S. has embargoed; or (ii) to any one on the U.S. Commerce Department's Table of Denial Orders or the U.S. Treasury Department's list of Specially Designated Nationals.

**TRADE SECRETS; TITLE:** You acknowledge and agree that the structure, sequence and organization of the Software are the valuable trade secrets of 3Com and its suppliers. You agree to hold such trade secrets in confidence. You further acknowledge and agree that ownership of, and title to, the Software and Documentation and all subsequent copies thereof regardless of the form or media are held by 3Com and its suppliers.

**UNITED STATES GOVERNMENT LEGENDS:** The Software, Documentation and any other technical data provided hereunder is commercial in nature and developed solely at private expense. The Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in this Agreement, which is 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov. 1995) or FAR 52.227-14 (June 1987), whichever is applicable.

**TERM AND TERMINATION:** The licenses granted hereunder are perpetual unless terminated earlier as specified below. You may terminate the licenses and this Agreement at any time by destroying the Software and Documentation together with all copies and merged portions in any form. The licenses and this Agreement will also terminate immediately if you fail to comply with any term or condition of this Agreement. Upon

such termination you agree to destroy the Software and Documentation, together with all copies and merged portions in any form.

**LIMITED WARRANTIES AND LIMITATION OF LIABILITY:** All warranties and limitations of liability applicable to the Software are as stated on the Limited Warranty Card or in the product manual, whether in paper or electronic form, accompanying the Software. Such warranties and limitations of liability are incorporated herein in their entirety by this reference.

**GOVERNING LAW:** This Agreement shall be governed by the laws of the State of California, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

**SEVERABILITY:** In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired and a valid, legal and enforceable provision of similar intent and economic impact shall be substituted therefor.

**ENTIRE AGREEMENT:** This Agreement sets forth the entire understanding and agreement between you and 3Com and supersedes all prior agreements, whether written or oral, with respect to the Software and Documentation, and may be amended only in a writing signed by both parties.

Should you have any questions concerning this Agreement or if you desire to contact 3Com for any reason, please contact the 3Com subsidiary serving your country, or write:

3Com Corporation, 5400 Bayfront Plaza, P.O. Box 58145, Santa Clara, CA 95052-8145 (408) 326-5000

This product contains encryption and may require U.S. and/or local government authorisation prior to export or import to another country.

# ISP INFORMATION

## Information Regarding Popular ISPs

Internet Connection Types	Characteristics	Popular ISPs
Dynamic IP (Clone MAC)	Cable modem ISP, non-hostname based. Need to clone MAC in the DHCP page of router.	MediaOne, RoadRunner, Optimum Online, Time Warner, Charter and Adelphia, Metrocast, RCN
Dynamic IP (Hostname)	Cable ISP, Requires Hostname to authenticate i.e. cx213818-B. Need to enter the hostname in the DHCP page of the router, exactly as it appears in your documentation.	@Home Network, Cogoco, ComCast, Cox, Excite, Rogers, Shaw, Insight, Videotron
PPPoE (DSL)	Usually special software installed on PC, MacPOET/WinPOET, EnterNet 300. The Cable/DSL Secure Gateway has this software built in and you can safely remove it from your PC. You will need to enter the account name and password that your ISP provided to you in the PPPoE page of the Gateway. Leave the service name blank unless your ISP requires it.	Bell*, Century Tel, Citizens, Primus, Prodigy, Snet, Sprint FC, Verizon, First World, Brightnet, Earthlink, Ameritech, Covad, Mindspring, Sympatico DSL, USWest, Qwest, SNet

Internet Connection Types	Characteristics	Popular ISPs
PPTP	Cable or DSL, always on. Some European ISPs require a PPTP tunnel to authenticate their network.	KPN (Netherlands), Austria Telecom
Static (DSL)	DSL Modem, always on. Need to enter ALL IP information from ISP in the "Static IP" section of the Gateway.	CableSpeed, Cnet, Direct Link, Drizzle, DSL Extreme, Earthlink Wireless, Fast Point, Flashcom, GTE-WhirlWind, Heavenet, HSA Corp, I-55, InterAccess, LinkLine, Mission, Nauticom, NAS, Omnitel, Onterra, Phatpipe, Rhythms, Speakeasy, Sterling, XO, Zyan
Static (Cable)	Cable Modem, Always on, ISP assigns specific IP information which needs to be entered on the "Static IP" page of the Gateway.	Cox Cable, Sprint, US Cable, Cable-Cable
* Bell includes Bell Advantage, Bell Canada, Bell South, PacBell and Southwestern Bell		



# GLOSSARY

## 10BASE-T

The IEEE specification for 10 Mbps Ethernet over Category 3, 4 or 5 twisted pair cable.

## 100BASE-TX

The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.

## 3DES

**Triple DES** (See DES). 3DES is an extremely secure encryption system that works by applying the DES encryption system three times on the same message using different keys. It is typically used in military applications where it is expected that the VPN traffic will be intercepted and an effort made to decode it.

## Auto-negotiation

Some devices in the OfficeConnect range support auto-negotiation. Auto-negotiation is where two devices sharing a link, automatically configure to use the best common speed. The order of preference (best first) is: 100BASE-TX full duplex, 100BASE-TX half duplex, 10BASE-T full duplex, and 10BASE-T half duplex. Auto-negotiation is defined in the IEEE 802.3 standard for Ethernet and is an operation that takes place in a few milliseconds.

## Bandwidth

The information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10 Mbps, the bandwidth of Fast Ethernet is 100 Mbps.

## Category 3 Cables

One of five grades of Twisted Pair (TP) cabling defined by the EIA/TIA-586 standard. Category 3 is voice grade cable and can only be used in Ethernet networks (10BASE-T) to transmit data at speeds of up to 10 Mbps.

## Category 5 Cables

One of five grades of Twisted Pair (TP) cabling defined by the EIA/TIA-586 standard. Category 5 can be used in Ethernet (10BASE-T) and Fast Ethernet networks (100BASE-TX) and can transmit data up to speeds of 100 Mbps. Category 5 cabling is better to use for network cabling than Category 3, because it supports both Ethernet (10 Mbps) and Fast Ethernet (100 Mbps) speeds.

## Client

The term used to describe the desktop PC that is connected to your network.

## DES

Data Encryption Standard. DES is one of the encryption protocols that can be used by an IPSec Virtual Private Network. It is a strong encryption standard only currently exceeded in security by 3DES.

## DHCP

**Dynamic Host Configuration Protocol.** This protocol automatically assigns an IP address for every computer on your network. Windows 95, Windows 98 and Windows NT 4.0 contain software that assigns IP addresses to workstations on a network. These assignments are made by the DHCP server

software that runs on Windows NT Server, and Windows 95 and Windows 98 will call the server to obtain the address. Windows 98 will allocate itself an address if no DHCP server can be found.

## DNS

**Domain Name System.** DNS allows Internet host computers to have a domain name (such as 3com.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "3com.com" into your Internet browser), the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.

## DSL modem

DSL stands for digital subscriber line. A DSL modem uses your existing phone lines to send and receive data at high speeds.

## Ethernet

A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks use CSMA/CD to transmit packets at a rate of 10 Mbps over a variety of cables.

## Ethernet Address

See MAC address.

## Fast Ethernet

An Ethernet system that is designed to operate at 100 Mbps.

## Firewall

Electronic protection that prevents anyone outside of your network from seeing your files or damaging your computers.

## Full Duplex

A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

## Gateway

A device that acts as a central hub by connecting to each computer's network interface card and managing the data traffic between the local network and the Internet.

## Half Duplex

A system that allows packets to be transmitted and received, but not at the same time. Contrast with full duplex.

## Hub

A device that regenerates LAN traffic so that the transmission distance of that signal can be extended. Hubs are similar to repeaters, in that they connect LANs of the same type; however they connect more LANs than a repeater and are generally more sophisticated.

## IEEE

**Institute of Electrical and Electronics Engineers.** This American organization was founded in 1963 and sets standards for computers and communications.



## IETF

**Internet Engineering Task Force.** An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.

## IP

**Internet Protocol.** IP is a layer 3 network protocol that is the standard for sending data through a network. IP is part of the TCP/IP set of protocols that describe the routing of packets to addressed devices. An IP address consists of 32 bits divided into two or three fields: a network number and a host number or a network number, a subnet number, and a host number.

## IP Address

**Internet Protocol Address.** A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with periods (full-stops), and is made up of a network section, an optional subnet section and a host section.

## IPSec

IPSec (Internet Protocol Security) is a VPN encryption protocol based on TCP/IP. It is a flexible protocol with a wide range of encryption options. IPSec is commonly used for both connections between separate private networks and for connections between remote PCs and private networks.

## ISP

**Internet Service Provider.** An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

## LAN

**Local Area Network.** A network of end stations (such as PCs, printers, servers) and network devices (hubs and switches) that cover a relatively small geographic area (usually not larger than a floor or building). LANs are characterized by high transmission speeds over short distances (up to 1000 metres).

## L2TP over IPSec

L2TP over IPSec is a combination of protocols commonly used to authenticate a user (L2TP) and encrypt data (using IPSec).

## MAC

**Media Access Control.** A protocol specified by the IEEE for determining which devices have access to a network at any one time.

## MAC Address

**Media Access Control Address.** Also called the hardware, physical or Ethernet address. A layer 2 address associated with a particular network device. Most devices that connect to a LAN have a MAC address assigned to them as they are used to identify other devices in a network. MAC addresses are 6 bytes long.

## NAT

Network Address Translation. NAT enables all the computers on your network to share one IP address. The NAT capability of the Gateway allows you to access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

## Network

A Network is a collection of computers and other computer equipment that are connected for the purpose of exchanging information or sharing resources. Networks vary in size, some are within a single room, others span continents.

## Network Interface Card (NIC)

A circuit board installed into a piece of computing equipment, for example, a computer, that enables you to connect it to the network. A NIC is also known as an adapter or adapter card.

## Protocol

A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

## PPPoE

**Point-to-Point Protocol over Ethernet.** Point-to-Point Protocol is a method of secure data transmission originally created for dial-up connections; PPPoE is for Ethernet connections.

## PPTP

**Point-to-Point Tunnelling Protocol.** PPTP is a simple VPN encryption protocol based on the Point to Point protocol. It is most frequently used to connect remote PCs to private networks.

## RJ-45

A standard connector used to connect Ethernet networks. The "RJ" stands for "registered jack".

## Server

A computer in a network that is shared by multiple end stations. Servers provide end stations with access to shared network services such as computer files and printer queues.

## Subnet Address

An extension of the IP addressing scheme that allows a site to use a single IP network address for multiple physical networks.

## Subnet mask

A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must assigned by InterNIC).

## Subnets

A network that is a component of a larger network.

## Switch

A device that interconnects several LANs to form a single logical LAN that comprises of several LAN segments. Switches are similar to bridges, in that they connect LANs of a different type; however they connect more LANs than a bridge and are generally more sophisticated.

## TCP/IP

**Transmission Control Protocol/Internet Protocol.** This is the name for two of the most well-known protocols developed for the interconnection of networks. Originally a UNIX standard,

TCP/IP is now supported on almost all platforms, and is the protocol of the Internet.

TCP relates to the content of the data travelling through a network — ensuring that the information sent arrives in one piece when it reaches its destination. IP relates to the address of the end station to which data is being sent, as well as the address of the destination network.

## Traffic

The movement of data packets on a network.

## VPN

**Virtual Private Network.** A VPN is a private network where the data is passed across a public network infrastructure such as the Internet. The data is kept private by using encryption.

## WAN

**Wide Area Network.** A network that connects computers located in geographically separate areas (for example, different buildings, cities, or countries). The Internet is an example of a wide area network.

## Wizard

A Windows application that automates a procedure such as installation or configuration.



# INDEX

---

## Numbers

100BASE-TX 87  
10BASE-T 87  
3DES  
    defined 87  
    upgrading to 63

---

## A

access rights 48  
adding special applications 50  
address  
    TCP/IP 73  
admin password 23  
    changing 34  
advanced settings 52  
alert LED 12  
Apple Macintosh. see Macintosh  
auto-configuration wizard 26  
Auto-IP addressing 75  
Auto-negotiation 87

---

## B

bandwidth 87  
BCIQ statement 99  
blocking Internet access 48  
broadband sharing 9

---

## C

cable specifications 78  
cable/DSL Ethernet port 13

cable/DSL modem  
    connecting to 17  
cable/DSL status LED 13  
category 3 cables 87  
category 5 cables 87  
changing the admin password 34  
client 87  
configuring computers 19  
configuring the Gateway 33  
configuring VPN 53  
connecting the cable/DSL modem 17  
connecting to the Internet 38  
Consignes importantes de sécurité 80  
creating a virtual server 46  
CSA statement 99

---

## D

data encryption standard 87  
daylight saving 62  
DES 87  
DHCP 87  
    recording settings 16  
    wizard 30  
DHCP Internet settings 41  
DHCP server  
    configuring 36  
DHCP settings  
    Macintosh OS 8.5/9.x 20  
    Windows 2000/XP 19  
    Windows 95/98/ME 20  
diagram  
    front panel 12  
    rear panel 13  
    sample network 9

- digital subscriber line 88
- disabling IPSec 56
- disabling PPPoE client software 20
- disabling the firewall 52
- disabling web proxies 21
- discovery application 71
- DMZ
  - virtual 46
- DNS 88
- domain name system 88
- DSL 88
- DSL Ethernet port 13
- DSL modem 88
- DSL status LED 13
- dynamic host control protocol 87

---

## E

- End User Software Licence Agreement 83
- Ethernet 88
- Ethernet port
  - cable/DSL 13
  - LAN 13

---

## F

- Fast Ethernet 88
- FCC statement 99
- feedback 8
- finding the Gateway 71
- firewall 9
  - defined 88
  - disabling 52
  - settings 45
- firmware

- upgrading 63
- front panel diagram 12
- full duplex 88

---

## G

- Gateway
  - changing the password 34
  - connecting the cable/DSL modem 17
  - defined 88
  - firewall 9
  - installation information 15
  - positioning 15
  - powering up 17
  - restarting 61
- Gateway configuration 33
- Gateway to Gateway connection 58
- getting help 33
- giving feedback 8

---

## H

- half duplex 88
- help menu 33
- hub 88

---

## I

- IEEE 88
- IETF 89
- installation information 15
- Internet protocol 73
- Internet Settings
  - PPTP 43

- Internet settings
  - blocking access 48
  - configuring 38
  - DHCP 41
  - PPPoE 42
  - static address 40
  - wizard 26
- inventory 11
- IP address 73
- IP defined 89
- IPSec
  - defined 89
- IPSec Routes
  - editing 60
- ISP defined 89
- ISP Information 85

---

## L

- L2TP 53
  - editing 59
- LAN defined 89
- LAN Ethernet port 13
- LAN settings
  - configuring 35
  - wizard 30
- LAN status LED 12
- LED
  - alert 12
  - cable/DSL status 13
  - LAN status 12
  - power 12
- loading Gateway configuration 62
- local area network 89
- login screen 23

- logs
  - viewing 64

---

## M

- MAC address 89
- Macintosh OS 8.5/9.x
  - setting up 20
- main menu
  - accessing 33
- media access control 89
- multiple hosts 51

---

## N

- NAT
  - configuring 43
  - defined 89
- network address
  - remote 57
- network address translation 43, 89
- network defined 90
- network interface card defined 90
- NIC defined 90
- notice board 34
- NTP server 62

---

## O

- one-to-many NAT
  - configuring 44
- one-to-one NAT
  - configuring 45

---

## P

- package contents 11
- password
  - changing 34
  - system 23
  - wizard 24
- PC privileges
  - setting 47
- PING
  - allowing 52
- port
  - cable/DSL Ethernet 13
  - LAN Ethernet 13
- positioning the Gateway 15
- power adapter socket 13
- power cycle 61
- power LED 12
- powering up the Gateway 17
- PPPoE
  - changing the password 38
  - defined 90
  - disabling 20
  - disabling client software 20
  - Internet settings 42
  - recording settings 16
- PPTP
  - defined 90
  - disabling 20
  - editing 60
  - Internet Settings 43
  - recording settings 16
  - users 53
- private IP addresses 75
- privileges

- setting 47
- product registration 8
- protocol defined 90

---

## R

- rear panel diagram 13
- recording DHCP settings 16
- recording PPPoE settings 16
- recording PPTP settings 16
- recording static address settings 16
- registration 8
- remote network address 57
- restarting the Gateway 61
- restoring Gateway configuration 62
- RJ-45 defined 90

---

## S

- safety information 79
- sample network diagram 9
- saving Gateway configuration 62
- server defined 90
- session chaining 51
- setting up
  - Macintosh OS 8.5/9.x 20
  - Windows 2000/XP 19
  - Windows 95/98/ME 20
- setting up computers 19
- settings
  - advanced 52
- setup wizard 23
- shared key 57, 58, 59
- sharing broadband 9
- special applications 49



- adding 50
- custom 50
- static address
  - recording settings 16
- static Internet settings 40
- status
  - viewing 64
- status LED
  - cable/DSL 13
  - LAN 12
- subnet mask 36, 90
- support 65
- switch 90
- system password 23
- system requirements 78
- system tools 61

---

## T

- TCP/IP 73, 89
  - defined 90
- technical specifications 77
- technical support 65
- time zone
  - setting 62
  - wizard 25
- traffic 91
- trigger port 51
- Triple DES 87
- tunnel shared key 57, 58, 59

---

## U

- upgrading firmware 63
- UTC (world time) 25

---

## V

- VCCI statement 99
- viewing status and logs 64
- virtual DMZ 46
- virtual private network 91
- virtual servers 45
  - creating 46
- VPN
  - configuring 53
  - defined 91
  - example 58
- VPN mode 53

---

## W

- WAN. See wide area network
- web proxies
  - disabling 21
- Wichtige Sicherheitshinweise 79
- wide area network 91
- Windows 2000/XP
  - setting up 19
- Windows 95/98/ME
  - setting up 20
- wizard
  - auto-configuration 26
  - defined 91
  - DHCP 30
  - Internet settings 26
  - LAN settings 30
  - launching manually 24
  - setup 23
  - summary 31
  - world time (UTC) 25



# REGULATORY NOTICES

---

## FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules, and the Canadian Department of Communications Equipment Standards entitled, "Digital Apparatus," ICES-003. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

---

## Information to the User

If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna.
- Relocate the equipment with respect to the receiver.
- Move the equipment away from the receiver.
- Plug the equipment into a different outlet so that equipment and receiver are on different branch circuits.
- Consult the dealer or an experienced radio/television technician for help.

The user may find the following booklet prepared by the Federal Communications Commission helpful:

### *How to Identify and Resolve Radio-TV Interference Problems*

This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4. In order to meet FCC emissions limits, this equipment must be used only with cables which comply with IEEE 802.3.

---

## CE Statement (Europe)

This product complies with the European Low Voltage Directive 73/23/EEC and EMC Directive 89/336/EEC as amended by European Directive 93/68/EEC.

---

## CSA Statement

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

---

## BSMI Statement

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

---

## VCCI Statement

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。





DUA08569-5AAA02  
Published November 2002